

Crypto-Asset Exchange Security Guidelines



The permanent and official location for Blockchain Working Group is
<https://cloudsecurityalliance.org/research/working-groups/blockchain/>

© 2021 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at <https://cloudsecurityalliance.org> subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Lead Authors:

Boulevard A. Aladetoyinbo, Esq.
Ken Huang
Dave Jevans
Abdulwahab AL-Zuaby

Blockchain/DLT Working Group Leadership:

Bill Izzo
Ashish Mehta
Jyoti Ponnappalli

CSA Global Staff:

Hillary Baron
Frank Guanco
Kurt Seifried
AnnMarie Ulskey

Table of Contents

1. Crypto-Asset Exchange Threat Modeling.....	5
Threat Models Against Exchanges	5
2. Crypto-assets Exchange Security Reference Architecture	7
3. Crypto-Asset Exchange Security Best Practices	11
3.1 Security Best Practices from End-User Perspective	11
3.2 Security best practices from Exchange Operator's perspective	15
3.3 Security Best Practices from Auditor's Perspective	24
4. Crypto-asset Exchange Administrative and Physical Security	29
4.1 Administrative Controls	29
4.2 Crypto-asset Exchange Legal Aspects	35
4.3 Insurance for Exchanges: Internal and External	38
4.4 Exchange Alliance for Security Incidents.....	43
4.5 Risk Management Process	44
4.6 Assigned Security Responsibility	46
4.7 Policies and Procedures	49
4.8 Information Access Management	53
4.9 Security Awareness and Training.....	55
4.10 Security Incident Management Procedures.....	56
4.11 Contingency Plan	58
4.12 Evaluation.....	59
4.13 Physical Controls.....	60

1. Crypto-Asset Exchange Threat Modeling

Author: Dave Jevans

Asset-Based Cryptocurrency-focused threat modeling framework capable of identifying such risks. ABC's key innovation is the use of collusion matrices. A collusion matrix uses a threat model to cover many threat cases while simultaneously managing the process to prevent it from becoming overly complicated. We demonstrate that ABC is effective by presenting real-world use cases and by conducting a user study. The user study showed that around 71% of those who used ABC were able to identify financial security threats, as compared to only 13% of participants who used the popular framework STRIDE.

The PDF download link is here <https://arxiv.org/pdf/1903.03422.pdf>.

This model is useful for analysing attacks against a cryptocurrency itself as well as analysing attacks against Decentralized Exchanges (DEXs) using smart contracts to control trading. However, for modeling against attacks on hosted wallets (e.g., cloud-based exchanges, OTC desks, cryptocurrency swap services), a more focused approach can be useful. Below we list a top 10 of the threats against exchanges.

Threat Models Against Exchanges

The types of attacks that we have seen against exchanges fall into these categories:

1. Phishing user credentials to gain access to cryptocurrency accounts and move money. These are sometimes combined with SMS hijacking to take over an SMS-based authentication code for a targeted user.
2. Technical attacks against an exchange to penetrate the internal system.
 - a. SQL injection attacks once an account has been created or accessed.
 - b. Vulnerabilities in software used to operate the exchange.
 - c. Unpatched software used by an exchange.
3. Spear-phishing of employees at an exchange in order to override controls on withdrawals
4. Spear-phishing of employees at an exchange to implant malware (particularly remote-access trojans) allowing attackers to access internal systems and hop between infrastructures.
5. Once access to internal systems is achieved, attackers often use internal APIs or access systems where there is insufficient access control between internal systems, so that they can move across the system. Attackers often use credentials stored on computers in the internal system to gain access to other systems.
6. Inadequate or incorrect use of cold wallet (offline) storage of private keys versus hot wallet (online) key storage used for day-to-day operations. 90% of an exchange's cryptocurrency should be stored in cold wallets that are not connected to the Internet. There needs to be a protocol for initializing cold wallets completely offline, for moving transfer requests between

the hot wallets and cold wallets (usually requiring a USB drive with signing instructions). Consider multisig for accessing cold wallets, requiring two employees to sign a transaction before funds are transferred from cold wallets to hot wallets.

7. Insider threats have been common in exchanges where employees gain access to hot wallet keys and copy them, gain access to cold wallet keys and copy them, or implant malware or remote access trojans on internal systems allowing them future access to these keys to steal crypto assets.
8. Decompiling exchange apps (iOS or Android) and discovering secret cloud API keys that are embedded in the app, then using those keys to access internal APIs which may be used to access hot wallets or user credentials.
9. Copying of wallet recovery keys. Exchanges need to protect their wallet recovery keys with even more protection than their hot or cold wallets. If an attacker gains a copy of the recovery keys, the entire assets of an exchange, including cold digital wallets, can be emptied. NEVER store recovery keys on electronic media. Store them written down on paper that is kept in a physical vault. There are metal physical devices that are more fireproof than paper.
10. Attacks against specific currencies which exploit vulnerabilities in the exchange's implementation: For example, many XRP (Ripple) implementations have a bug that allows for partial payments exploits. Suppose an exchange's integration with the XRP Ledger assumes that the Amount field of a Payment is always the full amount delivered. In that case, malicious actors may exploit that assumption to steal money from the institution. This exploit can be used against gateways, exchanges, or merchants as long as those institutions' software does not process partial payments correctly. <https://xrpl.org/partial-payments.html#partial-payments-exploit> In the first nine days of September 2020, the XRP holdings of 3 exchanges were wiped out completely.

2. Crypto-Assets Exchange Security Reference Architecture

Author: Abdulwahab Z

As the crypto-assets industry evolves, Crypto-Asset Exchanges (CaEs) increasingly push to cover landscapes that were, for decades, the private playground of financial service institutions—especially in enterprise environments/business ecosystems where DLT has much to offer (when suitably adopted) ushering enterprises into the future.

Crypto-Asset Exchanges exist in several formats; the polarized distinction between them revolves around their entity identification. Centralized Exchanges (CEXs) are owned and operated by known and identifiable entities that operate under the regulations of a jurisdiction – or across several. Decentralized Exchanges (DEXs) are, as the name suggests, virtually unbound -- except by choice -- to an entity (organization, jurisdiction) – yet some entities transacting on and across DEXs do not avoid jurisdiction anchoring to fortify legitimacy credence.

As reference architecture is a predefined architectural set/s of patterns that are instantiated, designed, and proven to function as prescribed in the context of its application; drawing parallels between CEXs and – for the lack of a better term – “conventional” financial services/systems “security” architecture, is not comprehensive nor practical on many levels beyond the basics of ICT and cloud security -- This is due to the redefinition of boundaries, actors and components inner workings pertaining to a crypto-asset exchange and its function beyond the headlines (order book, trade, swap, withdrawal, transaction, keys, etc.).

Crypto-asset exchanges are mediators between consenting entities; the mediation depth of complexity depends on the CEX enterprise architecture, business spectrum, and its scope-of-service; all combine – in addition to regulation where applicable – to dictate the extent of integration/interfacing needs to: crypto-assets networks, peer service providers as well as business support service providers such as KYC/AML, financial institutes, payment service processors, etc. Crypto-asset exchanges aspire to mediate transactions between entities using a hybrid set of assets that include government-issued fiat, public blockchain assets, wrapped/tokenized instruments, or combinations of the same.

Within this document, we will articulate a CEX reference architecture that applies to the broad spectrum of crypto-asset exchange types/formats as a generalized starting point for future CEX-type-specific iterations of the framework.

CEXs existence/business model revolves around rendering services that facilitate transacting instruments between interested parties (individuals or enterprises) in a manual or automated manner. These services vary in their parameters that constitute a transaction and its terms; thus, each configuration carries a product name (i.e., savings, derivatives, spot, staking, escrow, swap, futures, etc.).

The abstract services provided to entities revolve around a membership attained through varying levels of complexity or methods that span sign-up or crypto-keys (boomerang exchange, "anonymous" exchanges, web3.0, etc.) Membership is abstracted to be the transacting entity identifier coupling a member as an entity with the CEX, instruments claims, rights, duties, appropriation protection, etc.

Furthermore, CEXs services are delivered to members via applications that interface to core systems via API(s) and software clients; be it web/mobile apps or crypto wallets/DEX clients, as their GUIs/CLIs interact with the crypto-network via exposed/looped-back API endpoint servers or separate localized API daemons.

Thus, a CEX environment is one within which entities traverse available services via applications to *"Transact": conducting/executing actions and functions based on defined terms accepted by transacting parties.*

We have chosen this abstraction level, which entices the reader to zoom out and consider the big picture, corresponding security, and risk landscape. In turn, allowing for a holistic risk and mitigation dialog that identifies the requirements of a CEX regarding security programs, risk management, and operational policies; That is very critical, especially in an environment within which - not even CEX internal - a "Low Threat" zone is non-existent.

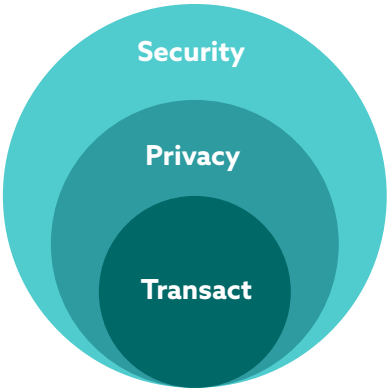


Figure 1

For CEXs to render their prescribed services, they require three main abstract blocks:

- A) Logic
- B) Instruments
- C) Integration

Each block scope covers its processes constituents [Code, Infrastructure, Staff], logic, and parameters of execution and governing how cross-block interactions, dependencies, inheritance flows natively via internal APIs middleware(s).

It is also worth noting that the Integration block extends to cover 3rd party systems and service providers that complement CEX functionality or facilitates it and offerings from peer entities, ticketing systems, and social media integration.

The following diagram visualizes the abstracted CEX described above and will be utilized as a reference architecture guide.

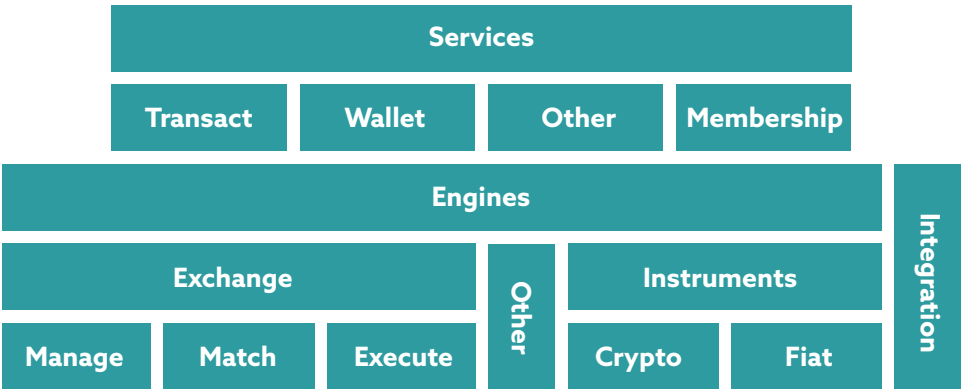


Figure 2. Crypto-asset exchange abstraction

It is important to note that "Other" in f:4 refers to services (by CEX, integrated 3rd party, or DLT networks) that are not core to the CEX as they are non-transactional. Such as vote, encrypt/decrypt messages, external balance tracking, dApps queries, etc. Or because they are externally executed by the member/DLT but may impact Member/CE standing (p2p swaps, mining/minting, token creation/swaps, Master/Service/Relay crypto-node management, wire-transfers, etc.).

A CEX goal is integral to facilitating transactions in an environment built for adopting Security & Privacy standards and best practices, which include traceability, trackability, accountability, and compliance. To apply to all transaction cycles and their milestones (i.e., request, start, cancel, reverse, etc.).

We will consider "transact" to be comprised of two distinctive, in-exclusive, interdependent scopes:

- A. **Value-Bound:** Transactions that actuate transfer of value such as deposit, withdrawal, charge, transfer, buy, sell, swap, dApp interactions, etc.
- B. **Value-Unbound:** Transactions or actions that do not directly transfer value -though they may be instrumental to the process- such as administrative processes, assignments of roles and rights, API routes, notifications, logging, dApp queries, etc.

Several frameworks exist for security and privacy (NIST, Jericho, OSA, SAMM, SDLC, PMRM ...) and architectures (SABSA, O-ESA ...). In the case of CEXs, the boundaries of their principle building blocks may be challenged if not redefined, but their merits hold.

The challenges of developing effective security/privacy architecture in the DLT realm magnifies how existing frameworks/models never quite fit one's situation and needs. The concepts of security/privacy architecture have many faces. Each framework has its focus and strength points with which Crypto-Asset Exchange can capitalize on by augmentation where needed.

To exemplify, f:3 and f:4 illustrate how the CEX terrain is and the contrasting security challenges in the CEX. These challenges can only be mitigated by a layered security and defense approach that considers the CEX and all its constituents as critical asset containers and "data" being the most vital asset at the core of each of those containers.

CEXs architecture must, at all levels, ensure that secure information exchange guidelines and best practices are adhered to and methodologies are enforced on bi-directional information flow streams before further actuation.

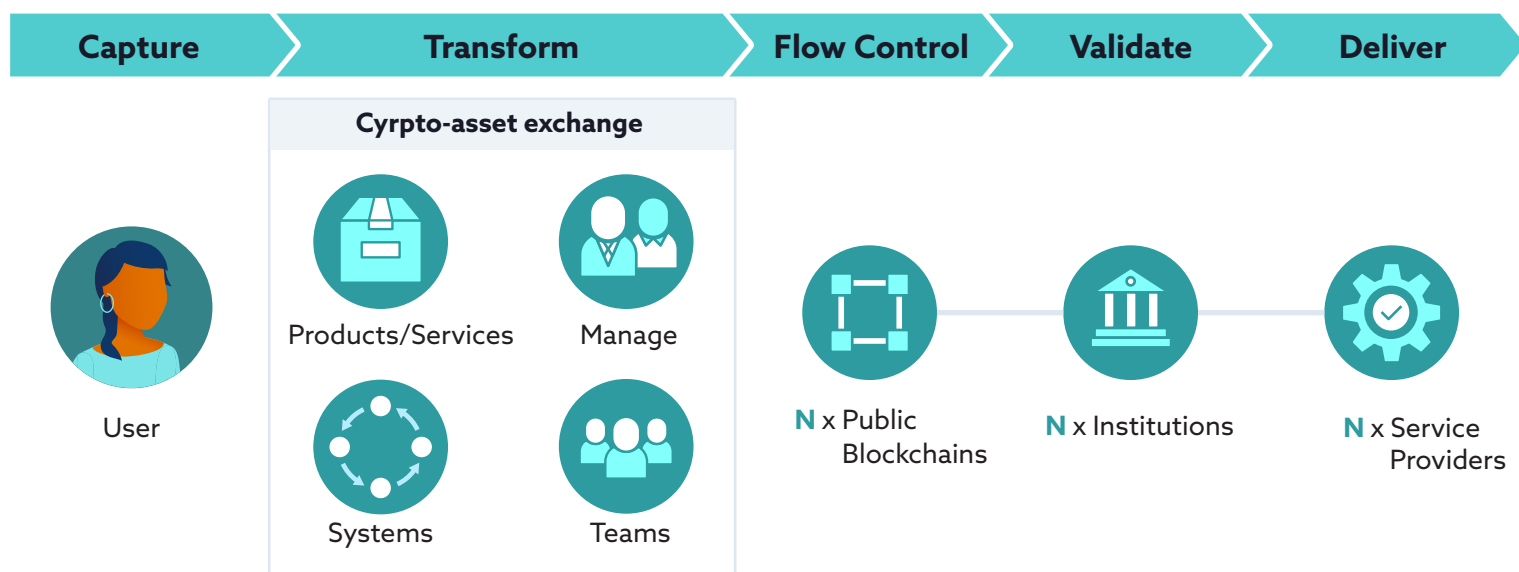


Figure 3. Crypto-asset exchanges: Centralized, Decentralized-Client and Public Blockchains

Centralized and hybrid exchanges should adopt a layered security approach to assert that every individual defense component has a backup to counter any flaws or gaps in other defenses of security. Separate layers in a multi-layered security approach focus on a specific area. These layers work together to tighten security and increase chances of breach prevention.

Falling back to the abstraction in centralized and hybrid exchanges, all transactions are to feed monitoring and response operation as well as policy management feedback streams with value-bound transactions having the highest sensitivity to alert threshold; value-unbound transactions are to be used to highlight/alert on anomalies that may indicate/imply occurrence of a malicious value-bound transaction.

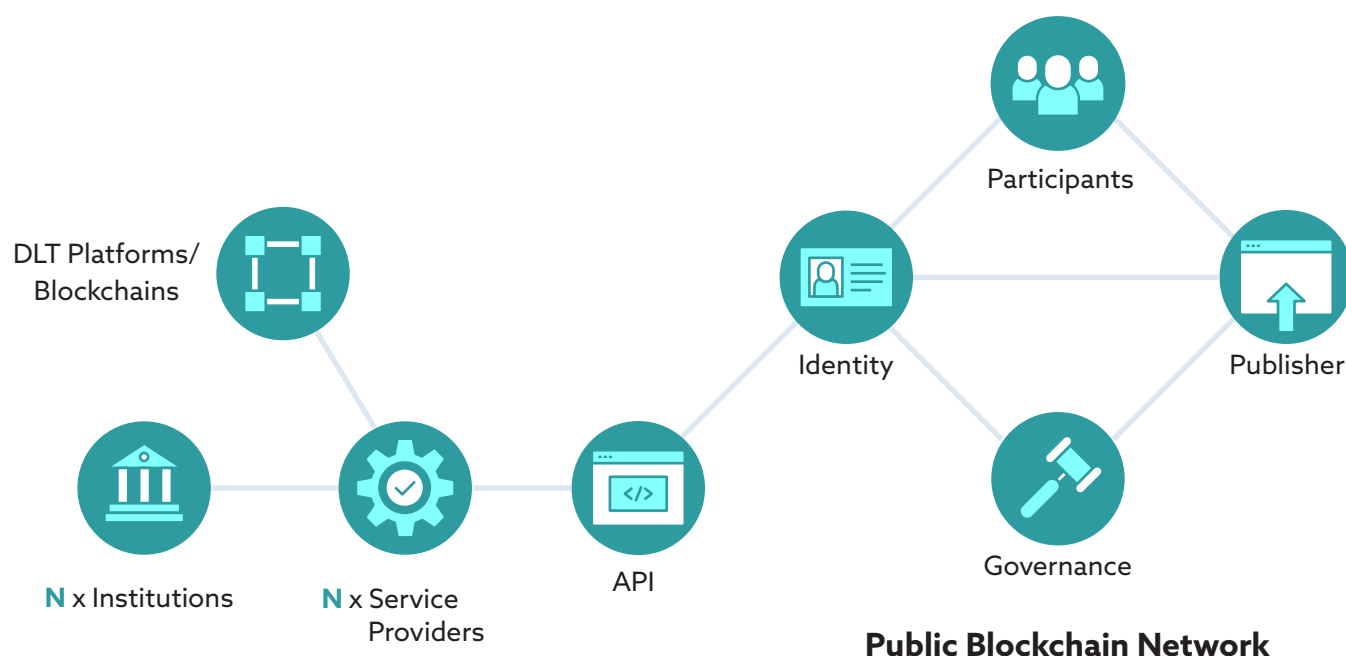


Figure 4. Decentralized Crypto-Asset Exchanges (dApp)

3. Crypto-Assets Exchange Security Best Practices

Author: Ken Huang

This chapter recommends security best practices from three different perspectives: end-user, exchange operators, and auditor perspectives.

3.1 Security Best Practices from End-User Perspective

1. Use reputable and safe exchanges

Avoid unscrupulous crypto-asset exchanges due to their potential lack of security measures, dishonest and scam business practices. Examples of scam practices include insider trading, pumping, and dumping schemes to profit from price changes due to its low liquidity, disabling withdrawal or deposit functions without justifiable reasons, and lack of internal security process enabling insider attack.

2. Password management and Two-Factor or Multi-Factor Authentication

Use a strong password with a minimum of ten characters and with a mix of upper case letters, lowercase letters, digits, and special characters. Enable two-factor or Multi-Factor Authentication authentication (do not use any exchange that does not support at least two-factor authentication). Use Google Authenticator instead of SMS as a second factor due to the possibility of SIM swap hijacking.

3. Use a separate device

If possible, use a separate device for the crypto-asset exchange and grant minimum rights. You can disable access to your photo album after completing KYC requirements. You can also disable its access to your contact list and again disable access to audio. You may still have to enable the exchange app to access your storage such that it can be updated regularly.

4. Understand the key concepts associated with wallet application

For Decentralized Exchanges (DEX), the client-side app usually holds a private key. The private key is used to sign a transaction that can withdraw funds from your wallet. It is important to fully understand the key concepts associated with the private key and what are their implications if you lose them.

Public Key and Address

In public-key cryptography, you have a keypair: the public and private key. You can derive a public key from a private key but cannot derive a private key from a public key. In Ethereum, the address “acts” like the public key, but it’s not the public key. In Ethereum, the public key is derived from the private key and is 128 hex characters. You then take the “SHA3” (Keccak-256) hash of this (64 characters); take the last 40 characters, and prefix with 0x, gives you your 42-character address.

Private Key

A private key is the secret half of your address/public key-pairing or a string of 64 hexadecimal characters.

(Almost) every string of 64 hexadecimal characters is a private key. This is the key you need to keep safe. Without it, you cannot access your funds.

Keystore File

A keystore file is an encrypted version of your private key in JSON format (though it does not have a JSON extension) or a fancy version of your private key protected by a password of your choosing.

Mnemonic Phrase (Recovery Phrase)

A Mnemonic phrase is another fancy version of your private key used to derive multiple private keys. Usually, a 12-24 word phrase that allows you to access an infinite number of accounts. Sometimes includes an extra 13th or 25th word chosen by the user for added security. It originated from Bitcoin Improvement Proposal (BIP) 39 Spec. The “derivation path determines the accounts you can access with this phrase.”

5. Be careful what you install or click

Avoid visiting unknown websites or downloading apps from untrusted sources. These sites and apps often host malware that will automatically install (often silently) and compromise your device. If attachments or links in the email are unexpected or suspicious for any reason, do not click on it.

6. Protect sensitive data

- Keep sensitive data (e.g., Social Security Number (SSN)), credit card information, student records, health information, etc.) off your devices with the exchange app installed.
- Securely remove sensitive data files from your system when they are no longer needed.
- Always use encryption when storing or transmitting sensitive data.

7. Keep your device secure

- Lock your device with a PIN or password - and never leave it unprotected in public.
- Only install exchange apps from trusted sources (Apple AppStore, Google Play).
- Keep the device's operating system up-to-date.
- Most handheld devices are capable of employing data encryption – consult your device's documentation for available options.
- Use Apple's Find my iPhone or the Android Device Manager tools to help prevent loss or theft.

8. Always use secure network connection

Avoid doing exchange transactions (buy/sell/deposit/withdraw/staking) over a public network. Any network other than your home or work network is an insecure network. Even though your device's data is encrypted, it is not necessary that the connected network transfers the data in an encrypted format. Moreover, there is a constant risk that the public network you connect with may be tapped, thereby proving a risk to the data being exchanged over the network. Before using any connection other than trusted networks, always ensure that you secure the connection using appropriate VPN settings.

9. Know different types of wallets and how to use them

There are four distinct categories of crypto-asset wallets: paper, hardware, cloud, and online.

Paper Wallets

Paper wallets are generally classified as cold storage. The term "paper wallet" generally refers to a physical copy or paper print of your public and private keys. Other times it means the software used to generate a pair of keys and a digital file for printing. Whichever the case, paper wallets can grant you a relatively high level of security. You can import your paper wallet into a software client or simply scan its QR code to move your funds. Although paper wallets are cold, they come with their share of risks, too. For instance, paper wallets can be easily damaged, burned, easy to copy, take pictures, and require mutual trust if you do not make one yourself. To make paper wallets less fragile, sometimes people laminate them, create multiple copies, store them in different locations, engrave them on pieces of metal or other sturdy materials, etc.

Note that it is a bad idea to keep electronic copies of your paper wallet on your PC. The private key of a paper wallet should always be kept offline. Keeping your paper wallet files online makes it as secure as a hot wallet.

Cloud Wallets

Your wallet, with Consider Centralised Exchange (CEX), is a form of cloud wallet. Your funds can be accessed using a cloud wallet from any computer, device, or location. They are convenient, but they store your private keys online and can be manipulated by exchanges. Therefore, they are more vulnerable to attacks and theft by design.

Software Wallets

Software wallets are downloaded and installed on a personal computer or smartphone. They are hot wallets. Both desktop and mobile wallets offer a high level of security; however, they cannot protect you against hacks and viruses, so you should try your best to stay malware-free. As a rule, mobile wallets are way smaller, more secure, and more straightforward than desktop wallets.

Hardware Wallets

Unlike software wallets, hardware wallets store your private keys on an external device like a USB. They are entirely cold and secure. Also, they are capable of making online payments too. Some hardware wallets are compatible with web interfaces and support multiple crypto-assets. They are designed to make transactions easy and convenient, so all you need to do is plug it in any online device, unlock your wallet, send crypto-assets, and confirm a transaction. Hardware wallets are considered the safest means of storing crypto-assets. Getting a hardware wallet directly from a manufacturer is the most secure way. It is unsafe to buy it from other people, especially the ones you do not know. Mind that even if you get a hardware wallet from a producer, you should always initialize and reset it yourself.

If we rank the security of different wallets, we can say that hardware wallet > paper wallet > software wallet > cloud wallet. Typically, it would be best if you store many of your crypto assets using a hardware wallet and only the funds you need to trade regularly with the exchange's cloud wallet.

10. Use Multisig for large amount of funds

Multisig stands for multisignature, a specific type of digital signature that makes it possible for two or more users to sign documents as a group. Therefore, a multisignature is produced through the combination of multiple unique signatures. Multisig technology has been extant within the world of crypto-assets, but the principle existed long before the creation of Bitcoin.

In the context of crypto-assets, the technology was first applied to Bitcoin addresses in 2012, which eventually led to the creation of multisig wallets. By using a multisig wallet, users can prevent the problems caused by the loss or theft of a private key. So even if one of the keys is compromised, the funds are still safe.

Imagine that Alice creates a 2 of 3 multisig address and then stores each private key into a different place or device (e.g., mobile phone, laptop, and tablet). Even if her mobile device is stolen, the thief will not be able to access her funds using only 1 of the 3 keys. Similarly, phishing attacks and malware infections are less likely to succeed because the hacker would most likely have access to a single device and key. Malicious attacks aside, if Alice loses one of her private keys, she can still access her funds using the other 2 keys.

Multisig is commonly used in a crypto-assets organization to manage corporate funds; it is recommended that individuals use this with family or friends as backup to avoid financial loss due to the theft or loss of a single key.

3.2 Security best practices from Exchange Operator's perspective

This section lists security best practices and associated technical security controls from the crypto-assets exchange's operator's perspective.

1. Distributed Denial of Service Attack (DDoS) protection

A DDoS attack exploits network vulnerability by flooding a server with malicious data packets requesting access. Overwhelmed by the influx of traffic, crypto-assets exchange servers end up crashing and disrupting services. Like most high-visibility businesses, crypto-assets exchanges have also been targeted with DDoS attacks. With the surge in interest and the resulting increase of traffic around crypto-assets, the door has been opened for bad actors to attempt to disrupt crypto-assets resources, denying users access. Defense measures against DDOS include the following:

Increase Network Bandwidth

Since DDoS attacks fundamentally operate on the principle of overwhelming systems with heavy traffic, simply provisioning extra bandwidth (such as a burstable bandwidth plan) to handle unexpected traffic spikes can provide a measure of protection. However, this solution can prove expensive as a lot of that bandwidth is going to go unused most of the time. What is more, additional bandwidth is not as effective at preventing DDoS attacks as it once was. These attacks are getting larger and more sophisticated, and no amount of bandwidth will be able to withstand attacks exceeding 1 Tbps without additional DDoS mitigation measures. Despite this provisioning, burstable bandwidth can help cushion the impact of an attack, providing the extra time needed to take action to combat the attack.

Use Early Detection and Packet Monitoring DDoS Attack Mitigation

There are various ways for IT security teams to monitor incoming traffic and identify the early warning signs vital to preventing DDoS attacks. Most routers support flow-sampling, which examines samples of incoming data packets to create a large-scale picture of trends in network traffic. However, since flow-sampling is only looking at a sliver of traffic at a time it can miss potentially damaging trends or turn up "false positives." Various Intrusion Prevention Systems/Intrusion Detection Systems (IPS/IDS) may be deployed to mitigate DDOS risk.

Manage and Block Malicious Traffic

Once exchange companies know a DDoS attack is underway, there are a variety of actions they can take to protect their infrastructure. The first strategy for preventing DDoS attacks is generally to stop malicious packets from reaching servers by "null routing" traffic, which drops and redirects requests flooding in under the direction of a botnet. DDoS optimized firewalls can also identify incomplete connections and flush them from the system when they reach a certain threshold. Routers can also be rated and help prevent the server from being overwhelmed. In some instances, all traffic is

diverted to a “scrubber” that sorts legitimate requests from malicious ones more thoroughly. Many of these cybersecurity measures, however, are bandwidth-dependent and could be overwhelmed by a large-scale attack.

Build Infrastructure Redundancy

As DDoS attacks become larger and more sophisticated, IT security efforts focus as much on backups and redundancies as on prevention. After all, if the goal of a DDoS attack is ultimately to disrupt service, it doesn't matter how a provider keeps its servers up and running as long as it stays online. Rather than meeting the attacks head-on, redundancy allows organizations to expand their infrastructure to make it more resilient. Redundancy also makes it easier to combat attacks actively as traffic can be cut off and rerouted more effectively.

Incorporate ISP Redundancy

Relying on a single Internet Service Provider (ISP) can leave a company vulnerable to DDoS attacks because any attack that disrupts the provider's systems will likely result in downtime for all connected systems. Moreover, when a DDoS attack is launched over a single ISP's connection, few solutions don't involve disconnecting and waiting until the attack is over. With a blended internet service that offers ISP redundancy, companies can design redundant networks that allow them to switch between different providers as needed during a DDoS attack.

Blocking DDoS Attacks With a Cloud Solution

Cloud DDoS providers can provide organizations with an extensive array of tools for combating DDoS attacks. Since they have much greater bandwidth capacity and more secure routers managing incoming traffic, data center security is better equipped to withstand attempts to overwhelm their infrastructure than the typical on-premises IT solution. Cloud Providers have the resources needed to combat the latest DDoS attack strategies with blended ISP connections that provide multiple layers of redundancy and real-time monitoring powered by predictive analytics and backed up by remote hands services.

2. Cross-Site Scripting (XSS-Protection)

Cross-site scripting (XSS) is a security vulnerability that allows a user to alter the code that an application delivers to a user executed in the user's web browser. It is most commonly found in web applications affecting the user's browser, and possible in other applications with embedded web content, such as an interactive «help» content viewer. When an XSS vulnerability is used as an attack vector, input sent by the attacker is insecurely processed within the application in a way that allows the attacker to alter the code sent to the victim and executed in the web browser.

To prevent this vulnerability, developers must validate all input to the application and encode all the information included in the output. This is an essential part of application development and will help prevent many different vulnerabilities, not just XSS.

More information about XSS and the protection against it can be found at [https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_\(XSS\)](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS)).

3. Do Not Expose Server Information

Showing back-end information about the server, software, and OS is not secure – you give the green light to hackers revealing secret information; if you are wondering why there is a quick link to Apache vulnerabilities list, Apache is still the most common web server in use. In each new release, developers fix those bugs and close the holes. https://www.cvedetails.com/vulnerability-list/vendor_id-45/Apache.html

4. Web Application Firewall

A Web Application Firewall (WAF) protects web applications from various application-layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others. Attacks to apps are the leading cause of breaches—they are the gateway to crypto-asset exchanges' valuable data.

5. Database Firewall

Centralized Crypto-Asset Exchange typically uses databases (SQL and No-SQL) to store user data, order books, transaction histories, administrative configurations, settings, etc.

Database Firewalls are a type of Web Application Firewalls (WAFs) that monitor databases to identify and protect against database-specific attacks that mostly seek to access sensitive information stored in the databases. Database Firewalls also enable monitoring and auditing all access to databases through the logs maintained by them. Generally, Database Firewalls are security-hardened appliances/software deployed either in-line with the database server (just before the database server) or near the network gateway (protecting multiple databases in multiple servers). Some database servers support host-based agents installed in the database server to monitor the local database events. But hardware-based firewalls support host/network monitoring without any additional load on the database servers. Both the hardware appliance and software agents can be deployed to work simultaneously, as well.

Since crypto-asset exchanges use databases to store critical financial information and the leak of the data will be catastrophic for the exchange, we highly recommend that database firewalls be leveraged to provide additional security measures for critical databases.

6. Third-Party Components and Patch

Usage of Third-Party Components (TPCs) has become the defacto standard in software development and has been applied for Crypto-Asset Exchange. These TPCs include both Open-Source Software (OSS) and Commercial-Off-The-Shelf (COTS) components. TPCs, used as pre-made building blocks, enable faster time to market and lower development costs by providing out-of-the-box functionality of standard functions, allowing developers to focus on product-specific customizations and features. While these TPCs are often treated as black boxes and are less scrutinized than comparable internally developed components, they are not without risk. Users inherit the security vulnerabilities of the components they incorporate. Historically, the selection and usage of TPCs is an engineering

decision, purely based on functionality. Given the increasing trend in the use of third-party components, security must be considered in the selection and usage of TPC. The number of vulnerabilities reported against TPCs, both OSS and proprietary COTS software, should serve as a strong testament that managing security risks due to third-party components is an essential duty for their users. Some good examples include Heartbleed (CVE-2014-01603), which was disclosed in 2014, and a security flaw in the GNU C Library (CVE-2015-75474) discovered by researchers in 2015. These vulnerabilities triggered analysis and remediation activities on an unprecedented scale that sent the software industry into a “patching frenzy.” TPCs are widely used in software development as an introduction and invitation to an unexplored land of opportunities to attackers. The current state of uncontrolled TPC usage must be replaced by a disciplined analysis and consideration of security risk.

For more information, please refer to NIST publication: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>.

7. Clickjacking Attack and X-Frame-Options

Using the SAMEORIGIN option to defend against clickjacking. X-Frame-Options allows content publishers to prevent their content from being used in an invisible frame by attackers. The DENY option is the most secure, preventing any use of the current page in a frame.

For more information about this security issue, please see <https://owasp.org/www-community/attacks/Clickjacking>.

8. HSTS (HTTP Strict-Transport-Security) and Secure Socket Layer (SSL)

HTTP Strict Transport Security (HSTS) is a web server directive that informs user agents and web browsers how to handle its connection through a response header sent at the very beginning and back to the browser. This sets the Strict-Transport-Security policy field parameter and forces those connections over HTTPS encryption, disregarding any script's call to load any resource in that domain over HTTP. HSTS is but one arrow in a bundled sheaf of security settings for your web server or your web hosting service.

How to Implement HSTS for your exchange website? If you employ subdomains in your content structure, you will need a Wildcard Certificate to cover HTTPS ONLY. Otherwise, you are pretty safe with a Domain Validated, Organization Validated, or Extended Validation SSL Certificate. Make sure you have these installed and working correctly. For more detailed information about enabling HSTS for your website, you will need to check with your hosting provider.

9. Applying Machine Learning for Better Protection

Machine learning technology has gained momentum in most major exchanges for security and fraud detection. The following are the primary uses of machine learning in crypto-asset exchange.

Flow Analysis

The flow analysis examines how funds are being transferred by known entities and comparing them to previously known data sets. Technology such as machine learning can be used to detect potential hack activities.

Address Classification

Classifying wallet addresses using machine learning is a method adopted by many exchanges. By identifying which wallet addresses are exchange wallets and different kinds of individual wallets, Exchange can block hacker's withdrawal of funds and protect users from being the victim of a scam. For example, for various YouTube "giveaway" scams, such as the recent scam from a Twitter hack, Coinbase was able to block the withdrawal of funds (<https://www.theverge.com/2020/7/20/21331499/coinbase-twitter-hack-elon-musk-bill-gates-joe-biden-bitcoin-scam>).

Analyzing Trading Behaviors

An innovative way of understanding how assets perform in the crypto-asset markets, recurrent neural networks are being used to understand better and predict the trading patterns of specific investors. In a given set of investors, this type of machine learning is used to identify investors in groups and discover how they invest their capital, the patterns they follow. This data can then be used to *accurately* predict how they will invest in the future. The predicate analysis is also to detect anomalies in trading behavior and potential hacker activities.

Fraud Detection

Machine learning uses a prevention system consisting of both machines and human analysts, supporting each other in a feedback loop. The machines start by being trained on well-known fraudulent patterns under various conditions, allowing them to generalize the knowledge and identify when similar patterns are found. The humans ensure everything stays accurate, and in doing so, make the machines better at identifying the correct patterns.

10. HTTP Public Key Pinning (HPKP)

HTTP Public Key Pinning (HPKP) is a security feature that informs a web client to associate a specific cryptographic public key with a particular web server to decrease the risk of Man In The Middle (MITM) attacks with forged certificates. It has been removed in modern browsers and is no longer supported.

To ensure the authenticity of a server's public key used in Transport Layer Security (TLS) sessions, the public key is wrapped in a X.509 certificate, usually signed by a Certificate Authority (CA). Web clients such as browsers trust many of these CAs, which can all create certificates for arbitrary domain names. If an attacker can compromise a single CA, they can perform MITM attacks on various TLS connections. HPKP can circumvent this threat for the HTTPS protocol by telling the client which public key belongs to a specific web server.

HPKP is a Trust on First Use (TOFU) technique. The first time a web server tells a client via a special HTTP header which public keys belong to it, the client stores this information for a given period. When the client revisits the server, it expects at least one certificate in the certificate chain to contain a public key whose fingerprint is already known via HPKP. If the server delivers an unknown public key, the client should present a warning to the user.

For information on how to enable HPKP, please refer to the following link: https://owasp.org/www-community/controls/Certificate_and_Public_Key_Pinning.

11. Use Hardware Security Module (HSM) Enabled Wallet

Hackers have successfully targeted Crypto-Asset Exchange's online hot wallet and stolen millions of dollars in the past (see Crypto Exchange Top 10 Security Risk, published by CSA GCR <https://www.c-csa.cn/mobile/news-detail/i-289.html>). Storing large sums of funds in cold wallets leveraging Hardware Security Module (HSM) and associated security operations becomes the top priority for exchanges of any size, large or small.

HSM is a physical computing device that safeguards and manages cryptographic keys and provides secure execution of critical code. These modules come in the form of a Peripheral Component Interconnect (PCI) card or an external rackable device that can be directly connected to the network. HSMs have built-in anti-tampering technology which wipes secrets in case a physical breach. They are designed around secure cryptoprocessor chips and active physical security measures such as meshes to mitigate side-channel attacks or bus-probing. These devices are heavily used in the banking industry and in all verticals where critical secrets must be protected.

The following is an HSM architecture recommended by Ledger, a company behind hardware digital wallet solutions:

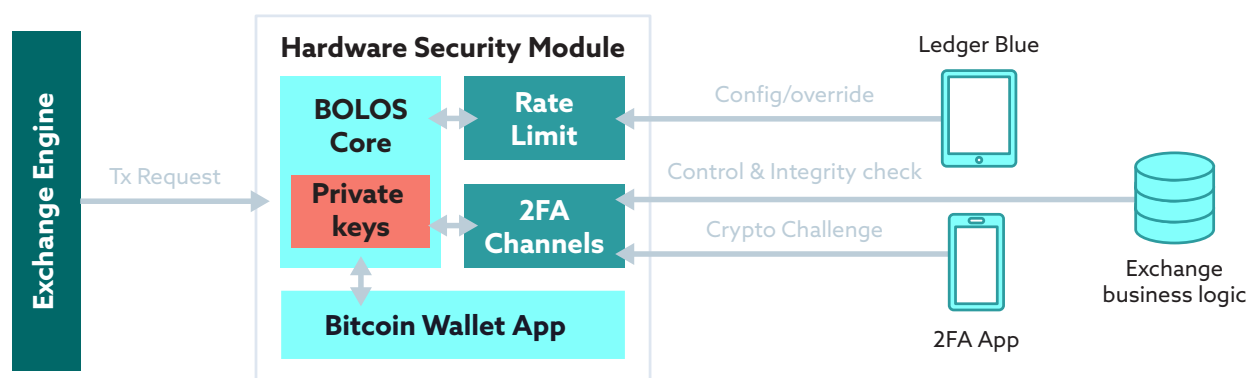


Figure 5. Decentralized Crypto-Asset Exchanges (dApp)

Here are the different modules/services in play:

Exchange engine: Requests payment orders (customer asks for a withdrawal).

Exchange business logic: Application Program Interface (API) with a view of all customer's balances, soft/hard withdrawing limits, and payment history.

Hardware Security Module: PCI card connected to a server in the exchange's data center (example: Safenet ProtectServer HSM).

Ledger Blue: Secure device protected by Personal Identification Number (PIN) code and kept in a safe. Accessible only by top management (CEO/CTO).

2-FA app: External second-factor channel on user's phone (containing an asymmetric key)
The HSM itself is architected around the following units:

Blockchain Open Ledger Operating System (BOLOS) core: The Ledger OS safeguarding the source from which all key-pairs are derived – exposing API so that internal business apps (such as a Bitcoin wallet or matching engine consistency check) can operate. Those apps are tested and signed offline and cannot be altered when the system is operating live.

Rate limiter: Sets hard limits on the velocity of what the HSM is authorized to sign (for instance: 1000 BTC / hour, 15000 BTC / day). This is a significant number and would ultimately decide the maximum amount of loss if the total system is compromised. The only way to modify the limiter's rules is through an authorization signed by the Ledger Blue device.

2-FA channel: The internal plug-in by which each signature request must be validated. It will require two challenge approvals: one from the exchange business logic ("send me your new business data so I can check if it is consistent with the previous system state"), and one from the user itself ("do you confirm that you want to do that?").

Bitcoin wallet app: Contains all the logic to build and sign transactions from an Unspent Transaction Output (UTXO) pool (could be replaced by an ETH wallet or any other crypto-asset).

For more information, please refer to the following link: <https://www.ledger.com/how-to-properly-secure-cryptocurrencies-exchanges/>.

12. Deploy a Zero Trust Architecture

A zero-trust architecture treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized. In essence, a zero-trust architecture allows full user access but only to the bare minimum they need to perform their job. If a device is compromised, zero-trust can ensure that the damage is contained.

The concept of zero-trust has been around for more than a decade; however the technology to support it is now moving into the mainstream. A zero-trust architecture leans heavily on components and capabilities for identity management, asset management, application authentication, network segmentation, and threat intelligence. Architecting for zero-trust should enhance cybersecurity without sacrificing the user experience.

For further reading, please see the following link: <https://threatpost.com/practical-guide-zero-trust-security/151912/>.

13. Error Handling

Error information and stack trace should not be displayed on the User Interface (UI) side. Hackers can obtain in-depth information about the application, database, and server information from error information. You can log unhandled errors that your code has not caught as most languages provide methods to do this (for example, .Net's `Application_Error` and JavaScripts global `on_error` handler). Any unhandled exceptions represent errors. Your code did not expect this; therefore, it could not recover or handle the situation gracefully. It is a good idea to log these so that you can fix the cause. This way, errors will not get thrown continuously as exceptions and should be exceptional. If they do happen, you want to know about them so you can catch and handle them.

14. 2FA

2FA is an extra layer of security used to ensure that people trying to access an online account are whom they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information.

Exchange developers should leverage Applications like Google Authenticator to enable two-factor authentication (2FA). You should avoid enabling SMS as a second factor as it is less secure than other software or hardware-based second factors.

15. 51% attack

A 51% attack refers to an attack on a blockchain (for example, ETC blockchain) by a group of miners controlling more than 50% of the network's mining hash rate or computing power. The attackers would prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins. They would almost certainly not be able to create new coins or alter old blocks.

Crypto-Asset Exchange can lose money if the hacker deposits the crypto-asset A at the exchange and trades it with another asset B and then withdraws the asset B and then launches a 51% attack on asset A.

There are at least four lines of defense against a 51% attack: The number of confirmation requirements can be increased. The attacking entity can be boycotted or, more drastically, the attacking entity can be attacked via a Distributed Denial of Service (DDOS) Attack, or there can be coding changes at the protocol level.

Because the attacker has to wait for the transaction to be confirmed before carrying out his double-spend attack, an easy solution to the double-spend problem would be to increase the number of confirmations before considering the transaction as fully completed.

This first line of defense is because although a 51% double-spend attack will succeed 100% of the time, the required waiting time and the monetary expenses of successful double-spend increase with each confirmed transaction. The greater the number of confirmations, the more blocks the attacker

needs to “reverse.” Thus the longer the required time and the more expensive it is to “catch up” and “overtake” the public ledger.

The effectiveness of this first line of defense depends on the time frame of a fuller response to the attacker. Theoretically, he can reverse even the oldest transactions if he consistently maintains 51% control. However, likely, any such control would only be temporary as these and other lines of defense are implemented. Therefore, increasing the number of confirmations would be the fastest and easiest response to a 51% double-spend attack.

This can be followed by a complete boycott of the attacking entity, which might sufficiently decrease the hashing power to below 51%. Any such boycott is likely to be permanent regardless of the reasons or the causes of the attack. Therefore, this line of defense is explicit and acted upon during an attack and an implicit threat to any profit-orientated entity.

Suppose neither is successful, depending on the attack’s time frame and protocol level reaction effectiveness. In that case, it’s been suggested that a DDoS could be possible on a theoretical level and that it would be immediately useful in lowering the hash rate of the attacker or at least slow them down; This would only be a temporary defense, however.

A fuller response to any such attack that would have the added long-term benefit of strengthening the protocol against such attempts may include tweaking the code to add resistance or thoroughly neutralize a possible 51% attack. This level of the response is still under research and hinges upon the actual implementation of blockchain. An exchange can now allow increased confirmation time for blockchain, which is more susceptible to 51% attacks such as ETC and Bitcoin Gold (BTG) than other blockchains.

16. Cloud Service Security Protection

Most Crypto-Asset Exchanges leverage cloud services such as AWS and Google Cloud for the server’s resources. It is vital to protect resources in the cloud by leveraging cloud security. Cloud security consists of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance, protect customers’ privacy, and set authentication rules for individual users and devices. . From authenticating access to filtering traffic, cloud security can be configured to the business’s exact needs. And because these rules can be configured and managed in one place, administration overheads are reduced, and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions. However, the implementation of cloud security processes should be a joint responsibility between the business owner and solution provider. For detailed information on Cloud Security and its critical focus, please refer to: <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf>.

3.3 Security Best Practices from Auditor's Perspective

The following table is proposed by a blockchain security company SlowMist.com as a recommended best practices or checklist for auditing exchange's security.

The latest update is at: <https://www.slowmist.com/en/service-exchange-security-audit.html>.

Audit Class	Audit Subclass
Open Source Intelligence Gathering	Whois information collection
	Real IP discovery
	Subdomain detection
	Mail service detection
	Certificate information collection
	Web services component fingerprint collection
	Port service component fingerprint collection
	Segment C service acquisition
	Personnel structure collection
	GitHub source code leak locating
	Google Hack detection
	Discovery of the privacy leaked
App Security Audit	App environment testing audit
	Code decompilation detection
	File storage security detection
	Communication encryption detection
	Permissions detection
	Interface security test
	Business security test
	WebKit security test
	App cache security detection
	App Webview DOM security test
	SQLite storage security audit

Audit Class	Audit Subclass
Server Security Configuration Audit	CDN service detection
	Network infrastructure configuration test
	Application platform configuration management test
	File extension resolution test
	Backup, unlinked file test
	Enumerate management interface test
	HTTP method test
	HTTP strict transmission test
	Web front-end cross-domain policy test
	Web security response head test
	Weak password and default password detection
	Management background discovery
Node Security Audit	Node configuration security detection
	Node data synchronization security detection
	Node transaction security audit
	Node communication security detection
	Node open-source code security audit
Identity Management Audit	Role definition test
	User registration process test
	Account rights change test
	Account enumeration test
	Weak username strategy testing

Audit Class	Audit Subclass
Certification and Authorization Audit	Password information encrypted transmission test
	Default password test
	Account lockout mechanism test
	Certification bypass test
	Password memory function test
	Browser cache test
	Password strategy test
	Security quiz test
	Password reset test
	OAuth authentication model test
	Privilege escalation test
	Authorization bypass test
	Two-factor authentication bypass test
	Hash robustness test
Session Management Audit	Session management bypass test
	Cookies property test
	Session fixation test
	Session token leak test
	Cross-Site Request Forgery (CSRF) test
	Logout function test
	Session timeout test
	Session token overload test

Audit Class	Audit Subclass
Input Security Audit	Cross Site Scripting (XSS) test
	Template injection test
	Third-party component vulnerability test
	HTTP parameter pollution test
	SQL injection test
	XXE entity injection test
	Deserialization vulnerability test
	SSRF vulnerability test
	Code injection test
	Local file contains test
	Remote file contains test
	Command execution injection test
	Buffer overflow test
	Formatted string test
Business Logic Audit	Interface security test
	Request forgery test
	Integrity test
	Overtime detection
	Interface frequency limit test
	Workflow bypass test
	Application misuse protection test
	Unexpected file type upload test
	Malicious file upload test
Cryptographic Security Audit	Weak SSL/TLS encryption, insecure transport layer protection test
	SSL pinning security deployment test
	Non-encrypted channel transmission of sensitive data test

Audit Class	Audit Subclass
Hot Wallet Architecture Security Audit	Who has access to the hot wallet? What is deposit and withdraw confirmation logic?
Private Key Management System Security Audit	Use of Hardware Security Module (HSM)? Where is it located? Who has access to it?

4. Crypto-Asset Exchange Administrative and Physical Security

Author: Boulevard A. Aladetoyinbo, Esq.

This chapter covers a wide range of administrative and physical security control measures for crypto-asset exchanges. These areas are:

- Administrative controls;
- Crypto-asset exchange operations legal aspects,
- Insurance (both internal and external),
- Exchange alliance for security incidents,
- Risk management process,
- Assigned security responsibility,
- Policies and procedures,
- Information access management,
- Security awareness and training,
- Security incident procedures,
- Contingency plan,
- Evaluation,
- Business associate contracts,
- Physical controls;
- Facility access,
- Workstation use,
- Workstation security,
- Device and media controls.

For emphasis, notwithstanding that there are three fundamental security control areas or taxons, which include management security, operational security and physical security controls, the chapter covers the essential administrative and physical security control areas for crypto-asset exchanges, and related crypto-asset exchange aggregator platforms.

See source URL: <https://www.lbmc.com/blog/three-categories-of-security-controls/>.

4.1 Administrative Controls

In a crypto-asset exchange context, administrative controls are controls requisite for operating and managing exchange activities, i.e., back-end operations and functions on the crypto-asset exchange infrastructure. But generally, administrative controls define the security system's human factors. All personnel levels within an organization are involved for user access determination, to what resources and information, by means such as:

- Personnel registration and accounting

- Personnel recruitment and separation strategies
- Disaster preparedness and recovery plans
- Training and awareness See URL:

<https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-sgs-ov-controls.html#:~:text=1.2.,-1.&text=Physical%20control%20is%20the%20implementation,Motion%20or%20thermal%20alarm%20systems>

Relevant and instructive to crypto-asset exchange administrative controls are the security objectives and control checklist contained in the ISO/IEC27002:2013 (referenced in “Blockchain and distributed ledger technologies – Security management of digital asset custodians” - ISO/NP TR 23576 ” (standard under development)). The ISO/IEC 27002:2013 referenced checklist includes the following:

3. Information security policies,
4. Information security organization,
5. Human resources security,
6. Asset management,
7. Access control,
8. Cryptography,
9. Physical and environmental security,
10. Operations security,
11. Communications security,
12. System acquisition, development, and maintenance,
13. Supplier relationships,
14. Information security incident management,
15. Business continuity management information security aspects, and
16. Compliance in that order.

It is recommended that crypto-asset exchange platforms consider for administrative and physical security purposes the ISO/IEC 27002:2013 checklist content items such as policies on information security, organization of information security, security of communications, security of human resources, security of operations, management of information security incident, asset management, access control, aspects of security for the continuous management of the crypto-asset exchange, compliance, acquisition of the system, development, and maintenance, et al.

The above list is instructive for information awareness practice adoption, implementation, and among others, by crypto-asset exchange platforms as part of the bedrock of their information security control objectives.

CEX, DEX and HEX as Crypto-Asset Exchange Infrastructure Configurations and Taxons

A crypto-asset exchange infrastructure can be configured in three ways i.e., as centralized , decentralized, and hybrid. A crypto-asset exchange infrastructure can be configured in three ways, i.e., as centralized, decentralized, and hybrid. However, a centralized crypto-asset exchange is a more popular and more mass-adopted crypto-asset exchange configuration than the other two taxons:

decentralized exchange and hybrid exchange. The peculiar configuration of a crypto-asset exchange influences the exchange infrastructure administrative and physical security considerations. This implies that a CEX comprises different administrative and physical security considerations than a DEX or a HEX, and vice versa.

It is further recommended that crypto-asset exchanges be somewhat taxonomized based on the technological architecture, nature, functionalities, characteristics, and reality of the crypto-asset(s) that they deal on could have economic, financial, social, legal, regulatory, and other implications.

1. Centralized Exchange (CEX)

This, unlike a decentralized exchange, is a custodial, centralized exchange platform that leverages databases (either SQL or NoSQL) for user data storage, management, maintenance, issuance, trading activities; clearing, settlement, custodying et al. CEX order books, bids, crypto-asset exchange transaction data history, market data, AML/KYC [data](#); customer private transaction keys, incidents, settings, configurations, etc., are centrally-controlled and administered on a centralized database server system. There is a list of more than 600+ centralized crypto-asset exchanges.

See source URL: <https://www.cryptowisser.com/exchanges/>.

2. Decentralized Exchange (DEX)

A Peer-to-Peer (P2P) decentralized crypto-asset exchange market infrastructure is built directly on a decentralized and distributed cryptographic ledger consensus algorithm the likes of Proof of Work (PoW), Proof of Stake (PoS), Distributed Proof of Stake (DPoS), asynchronous Byzantine Fault Tolerance (aBFT), etc. Unlike a CEX built on a centralized exchange matching engine, *sans* cryptographic consensus algorithm and platforming on a Distributed Ledger Technology (DLT) back-end.

Unlike the other crypto-asset exchange taxons, a decentralized exchange is nearly impossible to hack because it is normally spread across the globe. Furthermore, , because it has no centralized server database system. The spread of servers on nodes across the planet translates to lower risk, absolute server downtime absence, and virtual immunity to cyber-attacks. While centralized exchanges have been reportedly hacked and reported hacked from time to time, there has not been a reported decentralized exchange hack incident.

See source URL: <https://www.cryptowisser.com/centralized-exchanges-vs-decentralized-exchanges/>.

3. Hybrid Exchange (HEX)

This combines both the centralized and decentralized exchange value propositions and characteristics such as security and confidentiality in the case of a DEX and liquidity and functionality in a CEX. Though far less in use and adoption compared to CEX and even DEX, HEX is emerging.

For more on hybrid crypto-asset exchange operation and conceptual visualization, see source URL: <https://www.espay.exchange/hybrid-crypto-exchange-software> and the Legolas hybrid exchange structure diagrammatical works below available at another source URL: <https://decenter.org/en/hybrid-crypto-exchanges>:

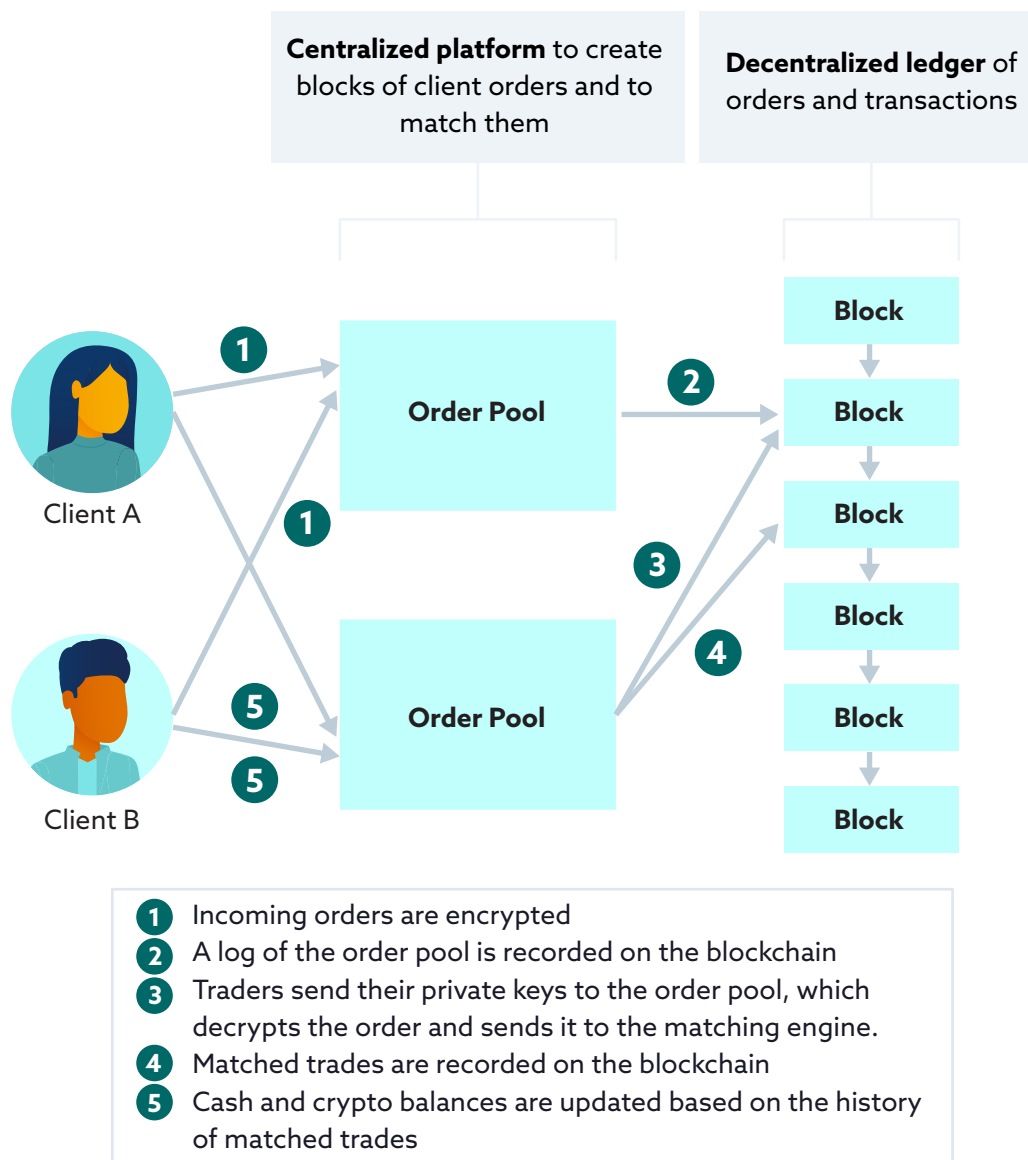


Figure 6

Crypto-Asset Exchange Infrastructure Configuration Differences and Features in Perspective

Centralized exchange (CEX)	Decentralized exchange (DEX)	Hybrid exchange (HEX)
Custodial (keeps custody of crypto-asset exchange transaction private keys)	Non-custodial (does not keep custody of crypto-asset exchange transaction private keys)	Both custodial and non-custodial (combines both features)
Built on the Internet Web 2.0	Built on the Internet Web 3.0 decentralized computing website application interface	Built both on the Internet Webs 2.0 and 3.0 decentralized computing systems
Keeps order book	Does not keep order book	Flexible
Not secure and confidential	Secure and confidential	"
More adopted	Less adopted	Far less adopted compared to CEX and DEX
High liquidity	Low liquidity	"
Non-disintermediated; not peer-to-peer; has a central authority or the Trusted Third Party (TTP)	Disintermediated; peer-to-peer; has no central authority; no Trusted Third Party (TTP)	"
Requires KYC/AML for compliance with local laws and regulations.	Does not require KYC/AML for compliance with local law and regulations (though KYC/AML regulations and programs can be baked into the underlying protocol by algorithmic automation of the regulatory logic into distributed ledger smart contracts)	"

Crypto-Asset Exchange Aggregator Platforms

Outside the basic crypto-asset exchange infrastructure configurations and taxons as a centralized crypto-asset exchange, decentralized crypto-asset exchange, and hybrid crypto-asset exchange, there exist aggregation platforms which are fundamentally crypto-asset exchange integration platforms that simplify user experience through a single unified common interface, and thus removes multiple log-in procedural difficulties across multiple crypto-asset exchanges.

These are also addressed and therefore caught by these security best practice guidelines as they fall within crypto-asset exchange information system appreciation, though outside the regular configurations and taxons.

See source URLs:

- <https://hedgetrade.com/what-are-dex-aggregators/>
- <https://coinmarketcap.com/alexandria/article/what-are-dex-aggregators-a-deep-dive-by-1inch>
- http://blog.ionixxtech.com/5_benefits_of_building_a_cryptocurrency_aggregator_platform/

Crypto-Asset Exchange Information Assets Security Level Assignments Based on 10 Security Aspects

Crypto-asset exchange must comply with and follow certain administrative security industry best practice standards, such as the RedTeam Security's open standard CryptoCurrency Security Standard (CCSS), which is a set of requirements designed to govern all information systems that store, accept or transact utility crypto-assets like Bitcoin, Ethereum, etc. The CCSS augments standard information security practices, and complements extant information system security standards like the ISO/IEC 27002:2013, PCI DSS, etc. Though the CCSS should be implemented by crypto-asset exchanges, as crypto-asset exchanges are information systems that store, accept and transact crypto-assets, additional security control safeguards should complement to secure the environments within which the crypto-asset exchange security management components operate.

1. Security Level Assignments

The CCSS, which is also used for system security consciousness scoring purposes, is a culmination that determines a crypto-asset exchange overall security compliance level on a scale of one to three. There are security levels from Level I, Level II to Level III described by the CCSS Steering Committee.

a. SECURITY LEVEL I Lowest crypto-asset security rating, though offers strong security measures for information assets proven by audit. The Level 1 security measure involves the use of industry-standard controls where information assets risks have been addressed.

b. SECURITY LEVEL II Controls used in Level 2 are also more enhanced and exceed the Level I strong security measures. Instances of this are organizations using decentralized security technologies that allow multiple signatures, which essentially provide redundancy if a key system or a person is compromised.

c. SECURITY LEVEL III The Level 3 is highest and offers the most comprehensive security measure. A crypto-asset exchange organization information system should demonstrate this security level. Demonstrating this security level means that the crypto-asset exchange has implementation of formal policies and procedures which are enforced within its business process purview at every intervening step, for the purpose to exceed enhanced security levels. The characteristics brought out in bold relief are multiple actor involvement requirements for critical actions, data authenticity protection via advanced authentication mechanisms, both

geographical and organizational assets distribution to minimise and mitigate to the highest degree possible, any chance of compromise.

















2. 10 Key Security Aspects

The 10 key areas addressed by the CryptoCurrency Security Standard (CCSS) include both hardware and software system components, personnel, policies, procedures, and more. These are:

1. Key/Seed Generation
2. Wallet Creation
3. Key Storage
4. Key Usage
5. Key Compromise Policy
6. Keyholder Grant/Revoke Policies and Procedures
7. Third-Party Security Audits/Pentests
8. Data Sanitisation Policy
9. Proof of Reserve
10. Audit logs

See source URLs: <https://cryptoconsortium.github.io/CCSS/>.

4.2 Crypto-Asset Exchange Legal Aspects

Cryptocurrency Security Standard	Level I	Level II	Level III
Key/Seed Generation			
Wallet Creation			
Key Storage			
Key Usage			
Key Compromise Policy			
Keyholder Grant/Revoke Policies and Procedures			
Third-Party Security Audits/Pentests			
Data Sanitization Policy			
Proof of Reserve			
Audit Logs			

Crypto-asset exchange operation legal aspects primarily entail the setting up in a jurisdiction for corporate personhood establishment purposes and compliance in that jurisdiction. At the moment, because of the nascence of decentralized cryptographic information systems, sparse regulation, pieces of legislation, and certain other factors across jurisdictions, there are crypto exchange

platforms that are virtually unregistered virtual organizations. The foregoing is more broadly coupled with the fact that crypto-asset exchange infrastructure solutions being Internet-based, are cross-border in nature, and therefore require not only national legislative and regulatory actions, monitoring and legal compliance frameworks, guidelines, policies, and standards, but as well as international standard-setting bodies' oversight function and cross-country collaboration. The issue of "pegging" the crypto-asset exchange infrastructure to a particular, known nation-state jurisdiction (not "digital jurisdiction") is a threshold question that must be taken into cognizance and resolved by a crypto-asset exchange. Though formalizing a crypto-asset exchange with legal personality is a fundamental question to which all crypto-asset exchanges must proffer answers, there are still other multi-layered questions that involve ongoing and active compliance with tax regulation, AML/KYC and CFT, etc. Crypto-asset exchange infrastructure legal aspects straddle crypto-asset exchange configurations and taxons as well.

A crypto-asset exchange platform in all its characteristics and manifestations must be compliant with the relevant legal aspects that affect it. A crypto-asset exchange infrastructure first instance fundamental, legal and operational aspects revolve around the following question areas hereunder:

1. Legal Entity Formation Question

The legal entity question concerns whether a crypto-asset exchange infrastructure is a virtually unregistered virtual organization (a.k.a. "unregulated exchanges"). If yes, it is not properly set up, and must therefore secure legal and compliance in a recognised legal jurisdiction with affordable and competent legal counsel assistance. And there are both national and international legal, regulatory and policy implications therefrom.

See source URL: <https://www.nortonrosefulbright.com/en/knowledge/publications/e383ade6/cryptocurrency-exchanges-and-custody-providers-international-regulatory-developments>.

The international aspect is germane because of the distributed ledger infrastructure cross-border nature, sometimes atop which the crypto-asset exchange information system is built. It is noteworthy that even centralized and hybrid crypto-asset exchanges, being Internet-based, have cross- and multi-jurisdictional presence as users can sign up to the system from different jurisdictions.

2. Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) Compliance

Due diligence requirements are prerequisite for a crypto exchange before onboarding a new user. The AML/KYC onboarding process is a *conditio sine qua non* for entry, irrespective of the jurisdiction where the crypto-asset exchange is incorporated. According to a [CipherTrace Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report](#), major trends and developments highlight a proportion of directly illicit funds received by crypto-asset exchanges have been halved, centralized crypto-asset exchanges like LocalBitcoins lead as go-to direct criminal funds for the third year in a row. Cross-border crypto-asset exchanges comprise three-quarters of exchange-to-exchange transfers, as US bitcoin users increasingly prefer high-risk exchanges for their crypto-asset transactional activities.

Crypto-asset exchanges in the Financial Action Task Force (FATF) member-countries must comply with the “[Travel Rule](#)” which required that Virtual Asset Service Providers (VASPs) obtain, hold, and transmit transaction originator and beneficiary information immediately and securely when conducting virtual asset transfers, to counter money-laundering and terrorist financing threats. Though not obligatory, it is both persuasive and advisable that non-FATF member-countries emulate this. The FATF virtual currency AML/CFT/KYC recommendations, standards, and reports on global efforts to combat money laundering and the financing terrorists should be taken into cognizance by crypto-asset exchanges. The FATF has issued several recommendations that seek to streamline crypto-asset exchange operations within the Travel Rule’s purview that is traditionally applicable to incumbent financial services industry actors. FATF Recommendation 16 principally requires that crypto-asset exchanges share customer transaction data between originator and beneficiary.

See source URLs:

- <https://fas.org/sgp/crs/misc/R43339.pdf>
- <https://getid.ee/aml-kyc-crypto-exchanges-wallets/>
- <https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/>
- <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>

3. Tax Compliance Consideration

Though many jurisdictions are yet to promulgate a comprehensive crypto-asset tax regulation regime, there are still tax obligations under extant tax statutes in most jurisdictions that must be complied with to a certain degree based on requisite dispensation. A quintessence of this is the US tax case-law authority *IRS v. Coinbase Inc.*, etc. Case No.17-cv-01431-JSC-2017. Crypto-asset exchange should endeavor to comply with these tax laws, pending laws to address the intrinsic peculiarities regarding adequate tax implication obligation fulfillment and compliance path for crypto-asset exchange business operations vis-a-vis their relevant information assets.

See source URL: <https://casetext.com/case/united-states-v-coinbase-inc.>

4. Suspicious Transaction Reporting (STR)/Suspicious Activity Report (SAR) Obligation

In the financial regulation vocabulary, the STR/SAR rationale is founded on the imperative necessity that financial institutions are obliged to file a report of potential, suspected legal violations. Though countries do have different decision criteria regarding when suspicious financial transaction reports must be filed, the general *conditio sine qua non* remains that transactions that do not make sense to a financial institution would be reportable. Furthermore, where a particular client is involved in an unusual transaction or purposed to obfuscate another separate transaction, reporting obligation would lie.

A crypto-asset exchange is obligated to report suspicious transactions on the exchange to the appropriate authorities, depending on their jurisdiction of origin or domicile, and international, bilateral, and or reciprocal treaties as both relevant and appropriate.

See source URL: https://en.m.wikipedia.org/wiki/Suspicious_activity_report.

5. Privacy Protection Regulation Compliance Obligation

Crypto-asset exchange operators are obliged to protect user private data on their platforms. Therefore, they have an obligation to comply with extant and emerging regulation in their home nation-state and regional or international data protection laws as found to be applicable based on informed facts and circumstances. Few examples of these are the European Union General Data Protection Regulation (EU GDPR), 5th EU AMLD and 6th EU AMLD etc.

6. Sanction Screening Control

Though sanctions screening is a control employed within traditional Financial Institutions (FIs) for detection, prevention, and sanctions risk management, it also extends to crypto-asset exchange infrastructures as they are considered an integral part of the Financial Market Infrastructures (FMIs). Therefore, sanctions screening compliance is required for crypto-asset exchange information systems.

The crypto-asset exchange user customer and name screening should be designed and primed for individual and corporate entity targeted identification onboarding and customer relationship lifecycle on the crypto-asset exchange financial market infrastructure.

See source URL: <https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf>.

4.3 Insurance for Exchanges: Internal and External

Internal and External Crypto-Asset Exchange Insurance Obligation

Centralized crypto-asset exchange platforms have been vulnerable and suffered several hack incidents in the past and present. There is no guaranteed solution or an end to possible future hacks. Therefore, the insurance policy strategy possesses the requisite potential to relieve any financial burden or insurmountable issues that may arise due to an exchange hack. Crypto-asset exchange and custodial storage platforms must insure both internally and externally against risks such as theft, third-party hack, fraud, spoofing, compromised API credentials, phishing software, brute force attack, malware attack, misappropriation, human error, wallet key loss, extortion through criminal means, unintentional data leakage, etc.

Exchange infrastructure crypto-asset liability insurance policy protection, customer fund insurance practices, and more, with crypto-asset exchange service providers being nascent at the moment, have almost next to no history, as there are many few and far between fragmented industry standards either under development or published, and being used by public sector actors and private sector actors, geared toward creating principles and guidelines to safeguard customer funds and grow crypto-asset exchange asset insurance practice culture among crypto-asset exchange service providers, users, institutions public and private.

As a minimum security standard protection measure, a crypto-asset exchange platform should self-insure by setting aside a portion of the exchange deposit to reimburse customers in any hacking incident. The Binance crypto-asset derivatives exchange [self-funded insurance](https://www.binance.com/en/blog/421499824684900373/Liquidation--Insurance-Funds-How-They-Work-and-Why-They-Are-Important-to-CryptoDerivatives-Part-2) scheme Secure Asset Fund for Users (SAFU) quintessence is relevant and recommendable as a standard crypto-asset industry practice for customer fund protection strategic purposes. A crypto exchange must imbibe, integrate and implement internal and external customer fund insurance best practice culture, as is the practice and standard for legacy non-crypto-asset exchange infrastructure models. An exchange can, outside self-insurance, create an insurance premium policy contract with an insurance institution, etc.

See source URLs:

- <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.forbes.com/sites/jeffkaufman/2019/09/05/lloyds-of-london-aon-and-others-poised-to-profit-from-cryptocurrency-hacker-insurance/amp/&ved=2ahUKEwikhl-7OfrAhVzqHEKH3wBNsQFjALegQIARAB&usg=AOvVaw1hD4nkg9JNgJuCSenhvPM&cf=1>
- <https://www.binance.com/en/blog/421499824684900373/Liquidation--Insurance-Funds-How-They-Work-and-Why-They-Are-Important-to-CryptoDerivatives-Part-2>

The insurance institution system and some of both internal and external crypto-asset exchange infrastructure information key pieces insurable are the **crypto-asset holder system (H)**, **insurer system (I)**, **Blockchain network (B)**, and **Crypto-asset exchange system (E)** separately carved out in bold relief below:

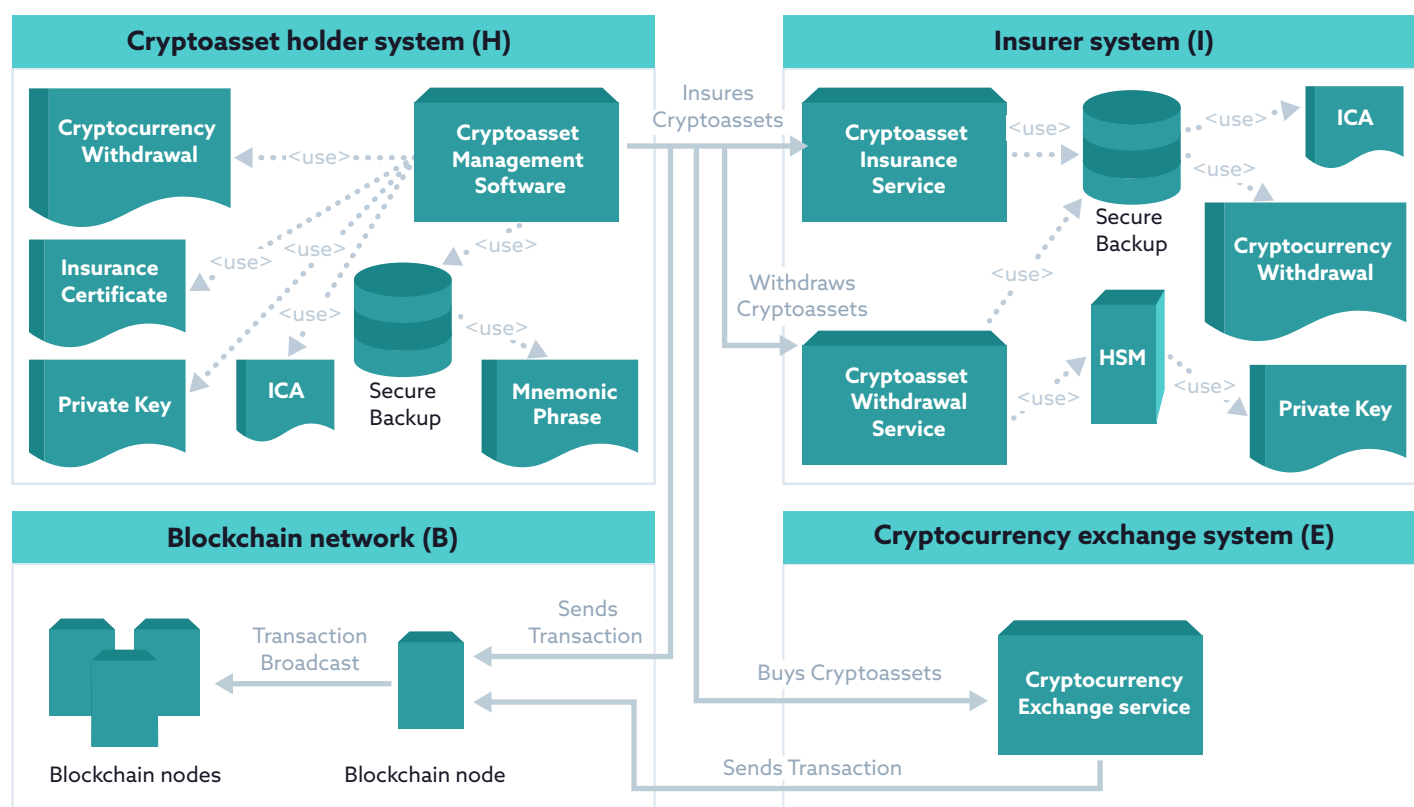


Figure 7. Crypto-Asset Exchange and Insurer System Interaction Diagram

Source URL: https://link.springer.com/chapter/10.1007/978-3-030-57805-3_4.

1. Blockchain Network (B)

This is a distributed ledger node aggregation system that consists of the network node totality, transaction broadcast, and transaction sending.

2. Crypto-Asset Exchange System (E)

The crypto-asset exchange system consists primarily of crypto-asset exchange services such as crypto-asset buying and sending transactions.

3. Crypto-Asset Holder System (H)

Consists of the components and activities such as crypto-asset withdrawal, crypto-asset management software, insurance certificate, secure back-up, private key, Independent Computing Architecture (ICA), mnemonic phrase.

4. Insurer System (I)

The insurance system consists of crypto-asset insurance service, database, ICA, crypto-asset withdrawal service, crypto-asset withdrawal, Hardware Security Module (HSM), and private key.

Crypto-asset, Hot Wallet, Cold Wallet, and Multisignature Wallet Insurance

Both extant and emergent insurance companies and institutions offer crypto-asset insurance services that cover crypto-asset, hot (online) wallet and cold (offline) wallet. One of such companies is the Lloyd's of London. Outside the above highlighted and diagrammed insurable crypto-asset exchange assets, other basic crypto-asset exchange insurable assets are:

1. Crypto-Assets

Crypto-assets are insurable cryptography-based assets that are insured against business and operational risks. But meeting crypto-asset exchange asset insurance requirement obligations created by regulatory body actions could prove to be a difficult task in the process. The reason for this possible difficulty on the part of crypto-asset exchanges is the lack of insurer capacity to provide competent crypto-asset coverage because of the absence of a better understanding of inherent and associated crypto-asset risks.

Going by the above, certain crypto-asset insurance service provider industry insiders and crypto-asset exchanges could fail to meet their insurance requirement obligations created by regulatory body actions. Another reason for this possible failure on the part of crypto-asset exchanges is the lack of insurers' capacity to provide proper crypto-asset coverage because of the absence of a better understanding of inherent and associated crypto-asset management risks. Adequate insurance provision to crypto-asset exchanges and crypto-asset trading companies in the traditional financial service sector player terrain would require insurers and their underwriters engage in massive-scale crypto-asset knowledge data investment acquisition quest.

According to policy and regulatory licensing scheme promulgation and announcements for crypto-asset exchanges in some jurisdictions, insurers and crypto-asset exchange brokers may not possess the requisite knowledge resources, experience, and proper crypto-asset information system for due compliance. The Hong Kong Securities and Futures Commission (SFC) crypto-asset exchange and crypto-asset investment firm licensing scheme requirements considered the following:

- i. Client crypto-asset custody.** A crypto-asset exchange operator is obligated to ensure substantial and active insurance policy risks coverage up to 95% for crypto-assets held in cold storage and full coverage for crypto-assets held in hot storage.
- ii. Insurance company choice data-driven decision criteria.** A crypto-asset exchange operator is required to use data-driven research, verifiability, and quantifiability as the fundament of its insurance company selection decision for crypto-asset exchange insurance policy. Attendant upon these is insured crypto-asset valuation schedule, maximum coverage per incident, overall maximum coverage, and any other factors exclusive to the occasion.
- iii. Settlement of claim arising out of a hacking incident.** Claims should be comprehensively settled by the crypto-asset exchange operator, an entity associated, or an insurance company. Customer claims arise out of hacking incidents on the part of the crypto-asset exchange associated entity due to a default.

See source URLs:

- <https://www.hedgeweek.com/2020/06/04/286220/crypto-exchanges-and-investments-firms-g-insurance-challenges-says-evertas>
- <https://news.bitcoin.com/the-difference-between-custodial-and-noncustodial-cryptocurrency-services/#:~:text=Custodial%20cryptocurrency%20services%20include%20most,your%20assets%20within%20their%20system>
- <https://www.internationalinvestment.net/news/4011749/lloyd-launch-crypto-insurance-services#:~:text=Insurance%20giant%20Lloyd%27s%20of%20London,price%20changes%20of%20crypto%20assets>

2. Online Wallet ("Hot Wallet")

Online storage wallet is connected to the Internet and is therefore completely online. Crypto-asset exchange should have a crypto-asset online wallet insurance policy scheme to safeguard and secure customer crypto-assets in their vault and storage online and compensate adequately in the event of a hack and related activities to prevent customer crypto-asset loss event.

There should be an extra level of caution, vigilance, and due diligence by crypto-asset exchanges when it comes to online wallet storage facility maintenance because of the online crypto-asset exchange storage system known and unknown vulnerabilities, risks, and threats, attacks like attack surface et al. Most "hot wallets" have no insurance coverage policies in place; therefore it becomes imperative that crypto-systems put in place an insurance cover for their online wallet infrastructures, and further as wallets online compared to wallets offline are less secure and more susceptible to hackers and technical vulnerabilities.

As part of its online wallet insurance strategy, a crypto-asset exchange should establish an insurance fund equivalent to the amount held in its online wallet for protection against customer crypto-asset fund loss, which may arise in the future, and thus affect the exchange operation and reputation both.

See source URL: <https://www.techriskreport.com/2020/04/cryptocurrency-insurance-for-hot-wallets/>

3. Offline Wallet ("Cold Wallet")

A cold storage wallet is the opposite of a hot storage wallet. Crypto-assets are completely kept offline when in cold storage and therefore not connected to the Internet in any way. A paper wallet should be used to create an offline storage wallet system having its private and public key pair to the token and never connected to the Internet unless for a specific purpose or purpose(s) through a USB device or any other means expedient to conduct a transaction, etc.

See URL:

- <https://www.bitcoin.com/get-started/setting-up-your-own-cold-storage-bitcoin-wallet>
- <https://www.coindesk.com/crypto-com-lands-record-360m-insurance-cover-for-offline-bitcoin-vaults>
- <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.forbes.com/sites/jeffkauflin/2019/09/05/lloyds-of-london-aon-and-others-poised-to-profit-from-cryptocurrency-hacker-insurance/amp/&ved=2ahUKEwikhl-7-OfrAhVzqHEKH3wBNsQFjALegQIARAB&usg=AOvVaw1hD4nkg9JNgJuCSenbvhvPM&cf=1>
- https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.financemagnates.com/cryptocurrency/exchange/bittrex-scores-300-million-in-crypto-insurance-from-lloyds-of-london/amp/&ved=2ahUKEwikhl-7-OfrAhVzqHEKH3wBNsQFjAOegQIBBAB&usg=AOvVaw2re_y6NQv5rL6nO_gFP6RV&cf=1

4. Multisignature Wallet (Multisig)

Wallet configuration that allows transaction authorization with private keys from more than a single entity. This is used mostly by crypto-asset exchanges to guarantee that exchange crypto-asset customer funds are protected even against any insider employee who may go rogue. Since the multisignature wallet storage medium holds crypto-assets, it is therefore insurable and should be availed insurance coverage against third-party hack, private key theft or any potential incident whatsoever. Crypto-asset exchanges should utilise multisignature wallet security enhancement capability, vis-a-viz non-custodial crypto-asset wallet.

A multisignature wallet account should be insured whole or insured to a certain degree amount contained therein. In a multisignature wallet insurance policy environment, different entities are keyholders and control transaction execution within the wallet. The crypto-asset exchange, the end-user, and the insurance company service provider are the keyholders. This creates a sufficient risk spread situation, adjustment, and risk transfer process that ensure crypto-asset multisignature wallet security and guarantee, as they make both technical and non-technical users have a sense of safety about their crypto-asset holding and free them from fear about a malicious crypto-asset hack or stolen crypto-asset fund barring any social engineering hacks from which they only have to be careful and cautious.

See source URLs:

- <https://www.coindesk.com/lloyds-backs-new-crypto-hot-wallet-insurance-scheme-from-coincover>
- https://link.springer.com/chapter/10.1007/978-3-030-57805-3_4
- <https://coincentral.com/bitcoin-insurance-policies/>
- [https://news.bitcoin.com/how-to-use-multisig-to-keep-your-coins-ultra-safe/#:~:text=Multi%2Dsignature%2C%20or%20multisig%2C,has%20applications%20for%20end%2Dusers.\(v\)https://www.google.com/amp/s/cointelegraph.com/news/civic-wallet-now-offers-1m-fdic-like-insurance-for-crypto/amp](https://news.bitcoin.com/how-to-use-multisig-to-keep-your-coins-ultra-safe/#:~:text=Multi%2Dsignature%2C%20or%20multisig%2C,has%20applications%20for%20end%2Dusers.(v)https://www.google.com/amp/s/cointelegraph.com/news/civic-wallet-now-offers-1m-fdic-like-insurance-for-crypto/amp)

4.4 Exchange Alliance for Security Incidents

Co-operation and coordination are useful tools that cryptosystems must deploy to prevent, mitigate, or altogether shut out possible attacks on a crypto-asset exchange. Crypto-asset exchanges should build industry alliances to forestall or manage security incidents. For crypto-asset customer fund and exchange infrastructure protection and security purposes, crypto-asset exchanges should collaborate to form industry alliances. This type of alliance and co-operative should foster unity among crypto-asset exchange operators, cybersecurity subject-matter experts, distributed ledger blockchain protocols, firms specialized in compliance for crypto-asset exchanges, and the likes. Further aim and objectives of this crypto-asset exchange alliance on security incident management should be to defend against outsider third-party attacks from bad actors and fraudsters, perennial potential risks, threats, and vulnerabilities crypto-asset exchanges (especially the centralized crypto-asset exchange platforms) are faced with. With decentralized crypto-asset exchanges and hybrid crypto-asset exchanges, the situation is somewhat different regarding risks, threats, and vulnerabilities. But altogether, no information system is immune from security incidents.

Some of the action steps through which industry collaboration effort against potential crypto-asset exchange attacks and security protection enhancement can work are by building decentralized incident report response system for intelligence gathering and sharing among crypto-asset exchange industry organization members to fight and stand against fraud, money-laundering, and other anomalies that plague the crypto-asset exchange infrastructure service marketplace. Tracking on-ledger transaction data history with aggregation algorithms, suspicious transaction monitoring, and blacklisting malicious crypto-asset transaction wallet addresses, etc., are useful strategies.

Collaborative effort fosters and engenders consensus and common security and protection standards among crypto-asset exchange industry players and helps preserve system integrity. As the crypto-asset exchange industry is an emergent growth area of competition, players should come together to build resilience, reputation, honesty, and integrity into the industry system. There should be a means to share and learn useful knowledge and information while not compromising each of their system operation's uniqueness that makes the industry competitive. Further features of such collaborative effort should be a defense-in-depth approach that enables monitoring, data-sharing, fraud detection, exchange on-chain/on-ledger data privacy, and confidentiality.

See source URLs:

- <https://www.binance.com/en/blog/421499824684900916/Cryptosafe-Alliance-Bringing-Better-Security-for-the-Crypto-Industry>
- www.cryptosafe.org

4.5 Risk Management Process

Crypto-asset exchange financial transaction dealing involvement precipitates and necessitates meeting with certain prerequisites to maintain the exchange operation integrity, safety, security, and keeping risk-free as much as possible. Financial operation risks pertain to volatility and certain other market risks, which a crypto-asset exchange would not be reasonably expected to bear for the exchange users. The below are the crypto-asset exchange risks and relevant crypto-asset exchange risks countermeasures:

1. Exchange Server Failure Risk

There exists the risk that servers serving a crypto-asset exchange operation are liable to fail so that the information system data may be lost and therefore no longer retrievable. Data center cloud storage system data leakage on foreign servers is also a potential data loss risk.

Exchange Server Failure Risk Countermeasure

The crypto-asset exchange must implement a data back-up contingency plan protocol to counter a crypto-asset exchange server failure risk. The data storage location should be separate, distant, and not dependent on the crypto-asset exchange server operations and activities. It is recommended that as a countermeasure, an exchange server failure risk should be spread and leveled out through every possible means attainable.

A back-up countermeasure and implementation plan should be made before the exchange operation starts, regular on-going updating and maintenance factored into both practice and consideration. Furthermore, regular back-up protocol checking to ensure quick data recovery on an incident's occasion is equally advised and recommended.

2. Exchange Regulatory Compliance Inability Risk

There are regulatory compliance requirements that a crypto-asset exchange must meet but may be unable to meet and become vulnerable to regulatory compliance risk. Regular compliance for crypto-asset exchanges is cross-border in nature as citizens and residents from various jurisdictions outside the exchange sovereign nation-state home may sign-on, use the exchange, and thus raise KYC/AML regulation compliance risk questions in the jurisdiction of the exchange user. In the light of this, local regulators and international standard-setters, and oversight functionaries have potential involvement. Non-compliance may cause site blockage and the centralized crypto-asset exchange fiat currency bank operation account closure by banks.

Exchange Regulatory Compliance Inability Risk Countermeasure

As a basic threshold question, it is recommended as a prerequisite minimum standard that the crypto-asset exchange must first be regulatory compliant with the local laws of its sovereign nation-state home where it primarily carries on its business operations. Compliance entails licensing, tax obligation fulfillment, etc. As we advance, compliance with international best practice standards such as investor protection, safety control, suspicious transaction manual verification, user identification, KYC/AML program requirements, etc., becomes essential in the process.

3. Exchange User Money/Funds Loss Risk

A crypto-asset exchange centralized runs customer funds loss risk, the exposure to which usually comes in the form of hacking, infrastructure access sans due authorization, theft, data leakage, insider job/compromise, third-party hack, human error, etc.

Exchange User Money/Funds Loss Risk Countermeasure

The exchange must ensure that customer funds are protected against every detail of inherent information system risks. Thus, concentrated protection measures against software and infrastructure vulnerabilities, bugs, and exploits must be implemented to fortify and make the system resilient against attacks, human errors, etc.

Other relevant countermeasure steps are putting in place stand-by quick incident response security management department team, training for developers to discern system vulnerabilities as quickly as possible, putting both internal and external security audit team to work, having a system administrator to monitor and investigate suspicious activities, enabling Two-Factor Authentication (2FA) functionality measure as an additional customer fund protection measure, exchange customer funds distribution in both offline and online wallets, etc.

4. Crypto-Asset Exchange Infrastructure Failure Risk

There are attendant issues upon withdrawals and trades on the exchange encountered due to demand and correlated growth increase. Therefore, occasion infrastructure failure risk is expressed as hacking risks, reputation loss risks, integration with third-party services risks, customer funds balance management risks, liability risks, etc.

Crypto-Asset Exchange Infrastructure Failure Risk Countermeasure

A crypto-asset exchange infrastructure can leverage scaling strategies and simulation tests as a failure risk countermeasure. Exchanges should use microservice architecture solutions for failure prevention on the infrastructure. The software algorithm implemented must permit changes to any of the services without affecting the entire infrastructure performance, and thereby increasing security level and guarantee uninterrupted infrastructure operation.

See source URL: <https://www.0hub.com/blog/crypto-exchange-risk-management#:~:text=Any%20exchange%20deals%20with%20financial,market%20risks%20for%20their%20owners>.

4.6 Assigned Security Responsibility

Notwithstanding the organization's role, all personnel are vulnerable to both technical and non-technical attacks, and therefore responsible for exchange security issues or security responsibility assignment. Crypto-asset exchange must take security responsibility assignment with no levity, as the entire information system architecture safety depends on the exchange security best practices. The exchange must build a "Defense in Depth" culture through multi-layer security control measures throughout the information technology system, where maximum security growth mindset permeates all aspects of the business processes. The exchange must consider vital exchange infrastructure security protection areas covering outages and attacks prevention, business continuity planning, automatic traffic encryption, traffic encryption control with Transport Layer Security (TLS), networks, application firewall capabilities, and other relevant information systems essential assets.

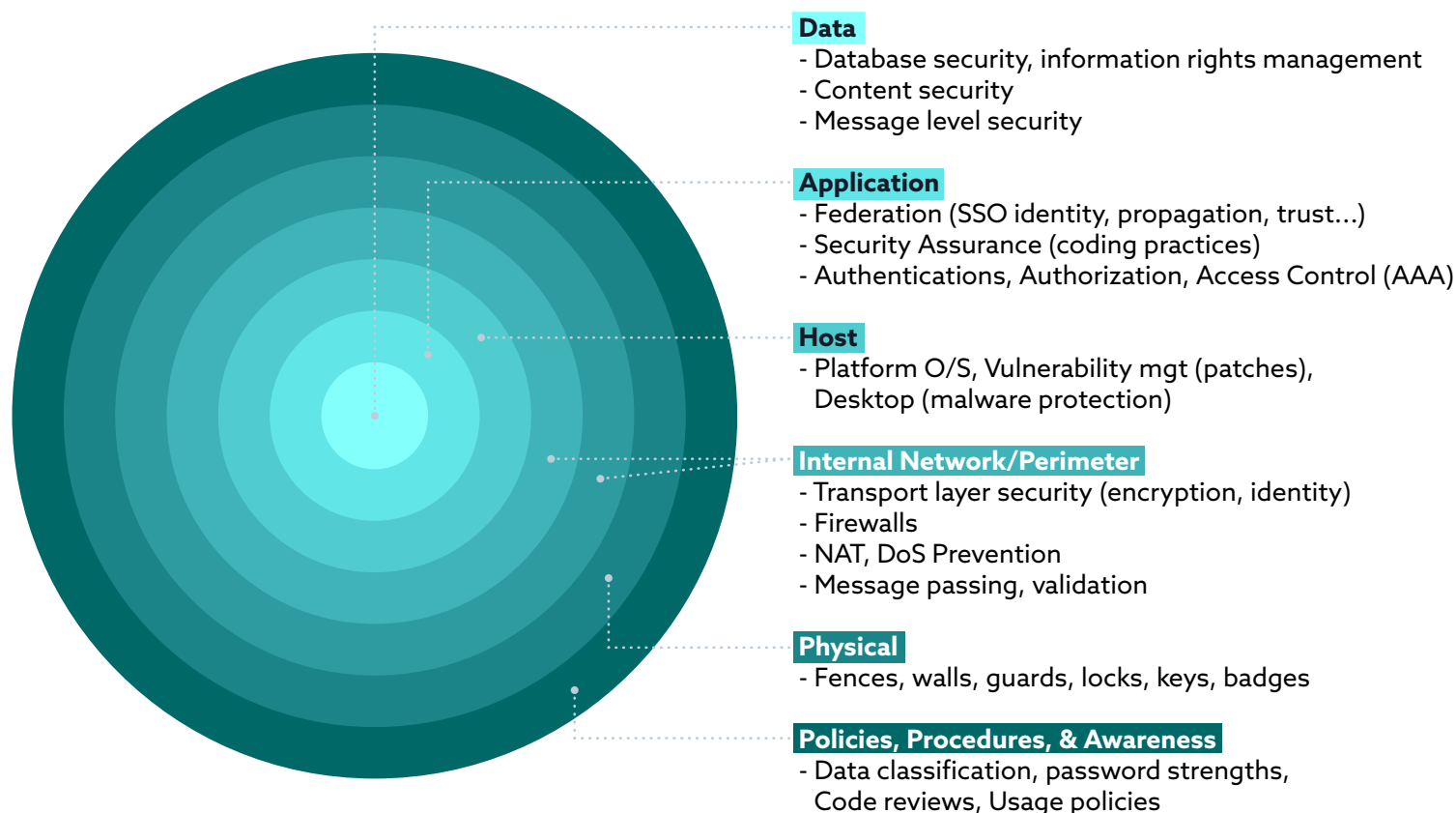


Figure 8

Regarding the crypto-asset exchange cybersecurity responsibility assignment, every exchange personnel must be involved. Ipso facto, an all-encompassing approach involving all aspects of people, processes, and technology would ensure cybersecurity best practice risk management and mitigation.

Exchange Personnel Security Responsibility Roles and Assignments

1. Executive Management Team

Chief Executive Officer (CEO) Selected by the Board of Directors (BoDs) and shareholders, the Chief Executive Officer (CEO) is the highest-ranking company executive member. The CEO's fundamental responsibilities entail major corporate decision-making, overall operation, and resource management while acting as the main information communication channel between the Board of Directors (BoDs) and corporate operations and the CEO interfacing with the public as the companies alter ego.

Since the CEO weighs so much influence in the organization, they have the power and responsibility to set the tone, vision and therefore foster an exchange organization cybersecurity best practice culture.

Chief Technology Officer (CTO)/Chief Information Officer (CIO) The Chief Technology Officer (CTO), as the highest executive technology position, usually reports to the Chief Executive Officer (CEO) and has crypto-asset exchange security responsibility roles, which entail taking care of Research and Development (R&D). The CTO roles further involve both short-term and long-term examination of the organization's technological needs and capital investment utilization strategy to attain the crypto-asset exchange organization's objectives.

Chief Information Security Officer (CISO) Since information security concerns come tops for business organizations, including crypto-asset exchanges, the Chief Information Security Officer roles, and responsibilities become strategically imperative for protection against information system security risks.

It is recommended that the CISO be saddled with the right security establishment and good governance practices, risk-free framework enablement, and scalable business operations in the challenging crypto-asset exchange business landscape.

Chief Operating Officer (COO) The Chief Operating Officer (COO), as a senior management team key member, reports to the Chief Executive Officer (CEO). It is recommended that the COO should shoulder the responsibilities of designing and implementing the exchange business strategies, plans, and procedures, alongside the establishment of policies that promote culture, vision while overseeing the crypto-asset exchange company operations, including the work of the executives; leveraging performance evaluation with analysis and interpretation of relevant data and metrics.

Chief Financial Officer (CFO) As part of the executive management team, the Chief Financial Officer should oversee the crypto-asset exchange company's financial security issues, analyze its financial strengths, and make requisite recommendations and improvements to overcome the shortcomings of identified financial weaknesses. The chief financial officer's job roles should be cashflow tracking, financial planning supervision involving capital investments, company capital structures, budgeting, forecasting, negotiations, and overseeing financial reporting matters.

Risk & Compliance Management Officer It is recommended that the Compliance and Risk Management Officer implement compliance policies and procedures, including the performances of regular internal reviews, to ensure that the crypto exchange is fully compliant with all laws and regulatory conditions.

The Risk & Compliance Management Officer's roles and responsibilities involve screening deposits and withdrawals with third-party analytics tools, to ensure KYC/AML compliance and monitoring of all transactions that go through the crypto-asset exchange system. These should further embrace withdrawal controls, which entail withdrawal requests screening for suspicious transactions and velocity to prevent possible fraud, and strict controls on funds access rights.

The Risk & Compliance Management Officer should also have roles such as providing certification and assessment opportunities for the crypto-asset exchange.

2. Development Team (Dev Team)

The exchange technology infrastructure development team should develop and oversee the source code deployment and operation, for the purpose to maintain source code logic and quality, while involving secure coding, and subjecting the code to peer review, adherence to the exchange Secure Software Development Lifecycle (SSDL), and using static source code analysis tools combination to achieve maximum security for the exchange.

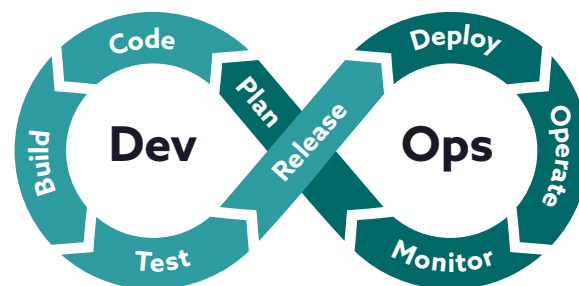


Figure 8

There must be crypto-asset exchange external audit certification for the smart contracts deployed on the exchange. The Two-Factor Authentication (2FA) must be implemented for transaction protection, password alongside biometric, e-mail verification, phone verification, and authenticator must also be implemented. Overseeing mandatory external address whitelisting through e-mail verification as part of the exchange transaction protection strategies should form part of the exchange security best practice measures.

The Development Team should be responsible for threat-modeling, penetration-testing the crypto-asset exchange information system infrastructure via many attack vectors, and outsourced third-party penetration-testing independent external auditing. This external and internal cybersecurity research expertise involvement has importance and potentials to ensure exchange information system infrastructure safety and security. The Development Team should have the responsibility to introduce and oversee detailed security assessment and evaluation measures like bug bounty campaign program cybersecurity best practice, the purpose for which will be to unearth and disclose vulnerabilities, exploits, and bugs having the potential to trigger compromise of the crypto-asset exchange system.

The evaluation and security assessment measures should further in detail entail the following:

- Threat modeling to ensure security controls completeness
- Risk control reviews to ensure effective privacy risk management best practice standard
- Certification and adherence to standards such as PCI:DSS 3.2.1 (payment card industry compliance requirement standard), ISO/IEC 27002:2013 (information security management), ISO/IEC 22701:2019 (privacy risk management), and CryptoCurrency Security Standard (CCSS); compliance requirement standard for a crypto-asset information system that includes decentralized web applications, crypto-asset exchanges, and crypto-asset storage solutions.

3. Computer Security Incident Response Team (CSIRT)

This is a stationed Information Technology (IT) professional personnel whose task and duty should be to provide the crypto-asset exchange organization with services and support, which surround the prevention, management, and coordination of potential cybersecurity-related emergencies. situations.

In any case that there is a data breach or any security incident on the crypto-asset exchange system, the CSIRT bears the responsibility to promptly respond to regain control and minimise damage through effective incident response and recovery assistance, and further to ensure prevention of future security incident recurrence.

See source URLs:

- <https://news.bitcoin.com/drawbacks-of-cryptocurrency-exchanges-how-non-custodial-services-are-the-solution/>
- <https://crypto.com/en/security.html>
- <https://www.sciencedirect.com/science/article/pii/B9780124199675000053>
- <https://aws.amazon.com/security/>
- <https://www.investopedia.com/terms/c/chief-technology-officer.asp>
- <https://www.roberthalf.co.nz/our-services/finance-accounting/cfo-jobs>
- <https://resources.workable.com/coo-job-description>
- <https://resources.workable.com/coo-job-description>
- <https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT>
- <https://www.bmc.com/blogs/ciso-chief-information-security-officer/>
- <https://www.synopsys.com/blogs/software-security/secure-sdlc/>

4.7 Policies and Procedures

There are certain standard emerging crypto-asset exchange industry practice steps implemented once or on an on-going basis new exchange customer onboarding. These form the basic keystone groundwork for exchange policies and procedures. It is standard that crypto-asset exchange platforms implement KYC/AML and set customer onboarding *conditio sine qua non*, or set relevant procedures. It is recommended that crypto-asset exchanges set procedures for onboarding a new user via various stages that the new prospective user must pass through and then be legally and regularly onboarded after due diligence requirements are met.

In order to issue, trade, clear, settle, send, receive, store or withdraw one's crypto-asset, etc., custodied on a crypto-asset exchange, the customer identity verification, and validation process requirement must be fulfilled. To this end, crypto-asset exchanges must put up a comprehensive KYC/AML program and set onboarding procedures. While there are many necessities for crypto-asset exchanges, including terms of use, customer protection, legal and compliance, and privacy policy, these exchanges must also have a full disclosure security statement that addresses how the crypto-asset exchange secures or plans to secure user crypto-assets within custodial exchange infrastructure protection obligations. In order to deter financial fraud and crime risks, crypto-asset exchanges must put customers through stringent due diligence measures. The customer onboarding

identity verification parameters should ensure that there are no criminal and money-laundering activities facilitated for bad actors who may attempt to leverage the exchange as a conduit.

Crypto-Asset Exchange Know Your Customer (KYC) Components

1. Policies

Exchange Privacy Policy/Policy on Acceptance/Onboarding Policy. There must be an adopted set of exchange privacy policy guidelines to -- among others -- guide client data collection, storage, custody, use, control, disposal, etc., under which an exchange manages customer PII. Crypto-asset exchanges should modify their privacy policies on an ongoing basis to reflect changes in their operations, new developments, and evolutions in law and regulation. They must duly notify the exchange users of these changes or amendments before they become effective.

The privacy policy should vividly describe information handling practices regarding service offerings on the exchange platform upon access and onboarding. Access and use of exchange should signify the use term acceptance. Information collected and processed by the exchange must comply with the limitations, relevant restrictions, and protection safeguards as contained in the applicable data privacy protection laws and regulations. Whenever user consent is required for PII processing, such user consent should be sought and obtained beforehand.

Following applicable laws, an exchange should obtain information about a user from time to time through third-party means, including those from public databases, credit bureaus, and ID verification partners. Due to the importance and sensitivity of this information, the crypto-asset exchange should, as part of third-party contract terms, require third parties to maintain appropriate physical, technical and administrative safeguards to protect the security and confidentiality of the personal privacy information entrusted to the exchange, or in the third party possession and dominion.

2. Procedures

Identification procedures. Crypto-asset exchange Know Your Customer (KYC) verification concerns stem from money-laundering and terrorist financing vulnerabilities considerations. Therefore, there are procedures for identifying a prospective customer at the entry-point regularly and overall through the customer lifecycle on the crypto-asset exchange platforms. These include identifying and verifying individual users via:

1. Personally Identifiable Information:
 - a. Full name
 - b. Birth date
 - c. Nationality
 - d. Signature
 - e. Gender
 - f. Utility bills
 - g. Phone number
 - h. E-mail address
 - i. Home address, etc.

2. Formal Identification Information:
 - a. National ID card
 - b. Tax identity number
 - c. Visa information
 - d. Passport number and all relevant pieces of information should be collected to ensure maximum adherence and compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) due diligence requirements.
3. Institutional Information:
 - a. Employer identification number (or equivalent government-issued)
 - b. Proof of legal formation (evidenced by corporate documents, i.e., Articles of Incorporation, Memorandum of Association, etc.)
 - c. All beneficial material, owners' personal identification information
4. Financial Information:
 - a. Bank account details
 - b. Payment card Primary Account Number (PAN)
 - c. Transaction history
 - d. Trading data, and/or
 - e. Tax identification means
5. Transaction Information:
 - a. Transaction originator information (i.e., name, etc.)
 - b. Transaction beneficiary information (i.e., name etc.)
 - c. Amount
 - d. Public blockchain transaction data hash analytics
 - e. Timestamp
 - f. Other transaction information-relevant data
6. Employment Information:
 - a. Office location
 - b. Job title
 - c. and/or role description
7. Correspondence:
 - a. Survey responses
 - b. Information provided to the crypto-asset exchange (exchange support team or user research team)
 - c. There should be different identification levels and stages to go through before onboarding a prospective crypto-asset exchange user; a sequence of actions or instructions to be followed, after each of which the prospective user moves up to the next stage, continues till the identity verification and validation exercise process completion. Personally Identifiable Information (PII) protection consideration should be made of paramount interest to crypto-asset exchanges since they are custodians of their customer's sensitive financial data, therefore have an obligation, and owe a fiduciary duty of care.

3. Risk Management

Handling, governing, controlling, directing, and maintaining the crypto-asset exchange custodial risks is the crypto-asset exchange operator's intrinsic role and responsibility, especially when the

entity hosts and signs crypto-asset transactions on behalf of the users with their exchange-hosted private keys. This situation may not be the same concerning a distributed ledger smart contract Decentralised Finance (DeFi) application like a Decentralised Exchange (DEX), where the users host their private keys locally and sign transactions, therefore, without having recourse to a Decentralised Exchange (DEX) for private key custodial access purposes each time for digital transaction signing, as obtainable in a Centralised Exchange (CEX) for instance.

4. Exchange Crypto-asset Transactions Monitoring

Transactions on the crypto-asset exchange should be monitored regularly and on-going as part and component of the Know Your Customer (KYC) due diligence requirement obligations. Monitoring transactions on the exchange entails exchange on-ledger/on-chain transaction data activities surveillance, detection of operation, and condition, keeping track and continual checking of transaction data inflow and outflow both on-ramp and off-ramp; crypto-asset to crypto-asset, fiat to crypto-asset, and *vice versa*.

5. Complaint Management Framework/Customer Support Services

A crypto-asset exchange must place a robust framework to manage customer complaints or a customer complaint support mechanism to attend to issues that affect customer activities and data protection and may be brought to the exchange notice at any material time. An exchange must always have stationed a Data Protection Officer (DPO) to the customer data protection end. Where a customer reasonably believes that their data rights have been infringed on, and thus lodges a complaint with the exchange internal customer service support mechanism, though such complaint could not be resolved, they must be allowed to have recourse to external, relevant data protection authority.

See source URLs:

- <https://www.google.com/amp/s/cointelegraph.com/news/memo-to-crypto-exchanges-kyc-compliance-can-be-a-competitive-advantage/amp>
- <https://www.google.com/url?sa=t&source=web&rct=j&url=https://readwrite.com/2020/04/20/know-your-customer-regulations-in-crypto-exchanges/amp/&ved=2ahUKEwjnfikmKXtAhVOD2MBHZ38CCoQFjAQegQIBhAB&usq=AOvVaw0GjcemPka9IEPD2YV1C6 &cf=>
- <https://www.google.com/amp/s/readwrite.com/2020/04/20/know-your-customer-regulations-in-crypto-exchanges/amp/>
- <https://cointelegraph.com/news/more-than-half-of-all-crypto-exchanges-have-weak-or-no-id-verification>
- <https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/>
- <https://www.coinbase.com/legal/privacy#:~:text=We%20will%20not%20use%20your,personal%20information%20with%20third%20partie>

4.8 Information Access Management

Identity and information access are intertwined and coterminous both. An identity and information access management system or strategy for a crypto-asset exchange must ensure that the right, appropriate, and designated people alone can access the crypto-asset exchange information infrastructure at any authorized and appointed time. As a policy and technology framework, a crypto-asset exchange should ensure that proper people for proper positions can have and maintain appropriate access to the exchange business enterprise assets and technology resources. The crypto-asset exchange system management requires tools and technologies for critical information user access control within the organization. Management of who has access to the crypto-asset exchange information system, when and how, is vital. This entails consideration and selection of the most effective and secure access authentication forms that the exchange organization needs, physical enablement, access restriction to various system information, and ability to monitor who is accessing, has access, or the kind of information that they access. These are all applicable, irrespective of the data storage facility in use, whether stored or replicated on a local or remote server or in the cloud.

Highlighted Risks

Employees with information access may change, share, or cause deleted sensitive files, such as payroll, personnel records, or confidential data of the company. Some of the other attendant risks are that employees can have unauthorized access to specific applications, and there can also be identity theft, extortion, sabotage, espionage, fraud, etc.

Authority Access Control (Management Power)

There should be a control of who can access the crypto-asset exchange different files, folders, and applications individually or on a group basis, i.e., via an Active Directory with Windows Server or other operating systems similar means. A quintessence is where all accounting department personnel have access to the exchange organization purchase ledger. Still, only those account personnel with additional access privileges can view the exchange organization payroll details.

In its information access management practices, a crypto-asset exchange must ensure the following:

- A systematic review of personnel information. Access and changing of privileges as and when due and necessary.
- Limitation of number and scope of personnel "administrator" rights.
- Careful consideration of access rights allocation, i.e., in a larger organizational context, is done on an individual role basis rather than on a person-to-person basis.
- Consideration for granting user accounts only privileges that are relevant to the user's work. An example is where a backup user needs not to install the software, but just run backups and backup-related applications. Any other privileges such as those which allow new software installation should be blocked (known as the "principle of least privilege").
- Consideration of the application of additional controls such as closely monitoring users with special access privileges.

- Employees should each have a unique user ID to log in with username and password authentication. The treatment of this should be like an office key or individual alarm code. It must not be shared or compromised in any way possible.
- On the question bordering on setting up a new employee record, it is integral that different people are involved in the process, including payroll arrangements and Information Technology (IT) access (known as "segregation of duties").
- When granting access rights to exchange employees who joined newly, switch roles, or move up the corporate ladder to a higher senior level, it's essential to consider carefully which access rights are granted.
- All the computers must be constructed to require secure log-in access, and log-out automatically if left unattended after a couple of minutes.
- User-access-right-privileges must be deleted immediately after they leave the exchange business information system formation.

Authentication Access Control

Where a user upon access right exercise identifies themselves via username and password log-in credentials, and thus implied that they have the authorization to access particular files, folders, or applications, they should have a prompt to prove that they are who they claim to be. Three essential identification proving methods exist:

1. Something or that which the user possesses, which may be a key, electronic token, a unique random encryption key, or a smart card.
2. Something that the user knows and memorizes, like a mnemonic phrase, password, Personal Identification Number (PIN), or even a father's name.
3. Something which could be a biometric scan, i.e., fingerprint, etc.

The deployment and use of the above factors complement considerably to confer sufficient confidence on the user identity claim for system-access-right purposes, especially using a more common password (but always advised to be a solid alphanumeric combination for stronger safety and security). Use of 2-Factor Authentication (2FA), 3-Factor Authentication (3-FA), and or Multi-Factor Authentication (3-FA) to safeguard confers more security and confidence because they could make the user impersonation for the purpose to gain access right more difficult.

More on password generally, the following is recommended to be observed by a crypto-asset exchange:

- The crypto-asset exchange information system must be set up so that it accepts only strong passwords for access and locks out attempts that use incorrect passwords to gain access.
- System default passwords must be changed to strengthen and harden access *conditio sine qua non*.
- Pre-determined regular interval password change enforcement.
- On the redundant piece of equipment disposal, it must be ensured that such redundant piece of equipment is securely cleared of password and username log-in credentials and all relevant confidential information.
- User education on password importance and social engineering risks.

Single Sign-On (SSO) Strategy

As part of its information access management best practices culture, it is highly recommended that a crypto-asset exchange consider the Single Sign-On (SSO) strategy, which is a centralised session authentication and user service where username and password log-in credentials are used to access multiple applications. The essence of this is, once signed on, access is granted to a myriad of services that enable the user to log in and out; without having to sign on again each time.

See source URLs:

- <https://www.csoonline.com/article/2115776/what-is-sso-how-single-sign-on-improves-security-and-the-user-experience.html>
- <https://www.google.com/amp/s/www.csoonline.com/article/2120384/what-i-iam-identity-and-access-management-explained.amp.html>
- <https://www.getsafeonline.org/information-security/information-access-management/>

4.9 Security Awareness and Training

Crypto-asset exchange should set in motion the necessary facilities to ensure training on security nuances and niceties, for, among others, to fortify against both internal and external attack vectors, which may negatively affect the crypto-asset exchange information system security. Security awareness training programs and materials on foundation and basics should have applicability to the exchange personnel without the risk of being generic, even as they match and reflect the crypto-asset exchange business values, goals, mission, and vision.

The basic, topical and typical areas that should be covered range from the exchange network security itself to privacy issues, social engineering attacks, other risks, potential threats, vulnerabilities, and relevant questions.

The exchange staff training program's security awareness and training drive should be two-fold, i.e., encompassing the exchange staff training program. Particularly training of the organization personnel and especially emphasizing keyholder-staff members on security consciousness, roles, and procedures because they possess and embody the crypto-asset exchange information access rights and, therefore, take action.

The other fold is organizing training and primary customer education on using and interacting with the crypto-asset exchange -- essentials for attaining conformant, emerging industry best practices. See URLs:

- <https://www.sciencedirect.com/book/9780124199675/building-an-information-security-awareness-program#book-description>
- <https://www.sciencedirect.com/topics/computer-science/workstation-security>
- <https://www.sciencedirect.com/book/9780128047545/cyber-security-awareness-for-ceos-and-management>
- <https://www.sciencedirect.com/topics/computer-science/security-awareness-program>

4.10 Security Incident Management Procedures

A crypto-asset exchange must have structured security incident management procedures and methodology to respond to and handle cyber-threat, breaches, and other security incidents that may happen in the crypto-asset exchange information system lifecycle. A clear-sighted Incident Response Plan (IRP) must address the threat or breach identified, damage effect minimization, cyber-attack cost reduction, and prevent possible future system attacks. There must be proper incident response procedures to limit a cyber-security incident impact; which procedures must be followed to the letter by the security teams who are faced with hectic IT environment activities during an incident. It is further recommended that a crypto-asset exchange, in addition to having a comprehensive incident response plan, should complete an incident response plan checklist. The development of an incident response policy is an effective strategy to complement before incident response plan deployment. It is standard practice that immediate cybersecurity incident reports be made by security analysts on discovery to promptly inform the relevant and concerned data subject parties and authorities.

There are privacy law provisions in privacy statute-laws, such as the California Consumer Protection Act (CCPA), which gives the consumers additional data privacy ownership control rights over their Personally Identifiable Information (PII) collected by businesses. The CCPA requires that public notification, and in some cases, personal statements be made to data subjects in the event of any cybersecurity incident taking place. The European Union General Data Protection Regulation (EU-GDPR) also grants similar rights to data subjects of Personally Identifiable Information (PII) data breach notification. There are similar provisions in other pieces of privacy legislation worldwide. Also relevant is the Payment Card Industry Data Security Standard (PCI DSS)--outlines in the payment card industry a set of requirements to ensure organizations having the responsibilities to process, store or transmit credit card data, have highly secure operation IT environment maintenance best practice culture in place, and therefore uphold highest data security and privacy standards.

1. Incident Response Plan Checklist Procedures

The crypto-asset exchange incident response phases should be a codification and encompassment of prerequisite steps for cybersecurity incident detection, reaction, scope, and inherent risks. Furthermore, there should be composite, thorough, quick response steps. Incident management response planned step by step avoids the usual haphazard scenario and organizational damage to brands and customers. The incident response plan should consider cross-business units and geographies and stakeholder communication regarding accidental risks, vis-a-vis the incident response security results.

ISO/IEC Standard 27035-1:2016 5-Step Procedural Outlines

The ISO/IEC Standard 27035 makes out a process that involves five steps when it comes to security incident management. These are the following:

1. Prior incident handling preparation
2. Potential security incidents identification *via* monitoring and reporting.

3. Identified incidents assessment to determine appropriate next steps for risk mitigation.
4. Incident response through containment, investigation, and resolution based on recognized incidents assessment.
5. Learning and documentation of the security incident key takeaways to aid in preparation for any future occurrences.

NIST Computer Security Incident Handling Guide (SP 800-61)

In a slightly different but equal breath as the ISO/IEC Standard 27035, this NIST Standard recommended incident response management steps and phases as follows:

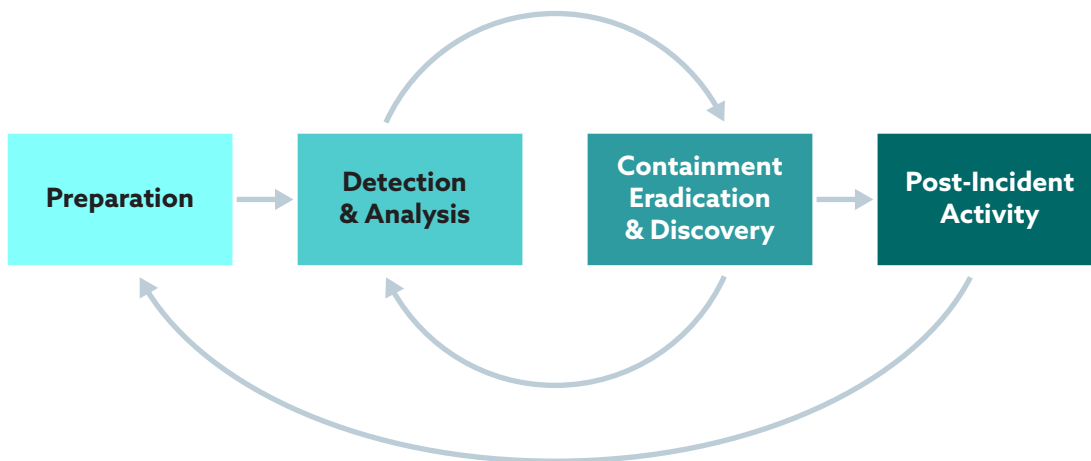


Figure 9: The NIST recommended phases for responding to a cybersecurity incident

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-Incident Activity

See URLs:

- <https://www.exabeam.com/incident-response/steps/>
- <https://digitalguardian.com/blog/five-steps-incident-response>
- <https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/>
- https://wou.edu/ucs/files/2015/11/WOU_Incident_Resp_Plan.pdf
- <https://www.bitlyft.com/what-is-security-incident-response-plan-2/>
- <https://oag.ca.gov/privacy/ccpa>
- <https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-proces>

4.11 Contingency Plan

With the perennial crypto-asset exchange cyber-attacks and hacks, crypto-asset exchange (centralized, decentralized, and hybrid) must have comprehensive cybersecurity Contingency Plan arrangements, i.e., written risk management document which contains instructions, considerations, and recommendations for the crypto-asset exchange about its information system infrastructure security practices, to protect from emergency, disaster and data recovery during a data security breach incident, or system disruption. It is recommended that the crypto-asset exchange has a basic crisis management plan and conduct, thereon a regular crisis drill or simulation on an on-going basis, as part of its contingency planning arrangements.

The NIST guidelines *Contingency Planning Guide for Federal Information Systems* (NIST SP 800-34) is both instructive and relevant in helping companies and organizations develop well-laid out, practical information system contingency plans. There are distinct cybersecurity contingency plan component areas, which must be addressed in the crypto-asset exchange information system. These are:

1. Disaster Recovery Plan

These are written and documented procedures and strategies that guide how to recover and protect the information system after a cyber-attack incident or natural disaster or any significant system disruption. In the Information Technology (IT) environment, this is implemented by the restoration of the information systems and applications of crypto-asset exchange from an alternative information storage system, i.e., a site designed for emergency purposes.

2. Emergency Mode Operation Plan

A Business Continuity Plan, having the primary focus for listing guidelines and procedures for everyday business operations sustenance during and after a security breach incident, i.e., emergency, disaster, or disruption of the crypto-asset exchange information system. EMOP potentially encompasses systems and operations having support requirements. More often than not, the shortcomings are that EMOP usually has short-term plans for business continuity processes, but not long-term continuity and recovery processes. EMOP has such effects as risk mitigation and system critical asset loss risk reduction in cyber-attacks such as ransomware invasion etc.

3. Data Backup Plan

A comprehensive contingency plan definition exists already regarding how the crypto-asset exchange operator should operate during critical information assets cyber-attacks. However, it is recommended that an effective data back-up plan for rapid service restoration post-cyber attacks should be put in place.

4. Disaster Recovery Plan (DRP)

This plan quickly redirects data and information into the storage system as a post-disaster recovery measure. As part of the larger whole Business Recovery Plan (BRP), the DRP is crucial. The crypto-asset exchange operator requires the DRP to achieve and maintain their crypto-asset exchange information service infrastructure equilibrium.

Disaster event classification, though not exhaustible, based on the information system type uniqueness, straddles natural consequences of wide scoping and occasioning detrimental damage.

See source URLs:

- <https://study.com/academy/lesson/cybersecurity-contingency-plans-purpose-development-implementation.html>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7149346/>
- <https://www.financemagnates.com/cryptocurrency/news/nydfs-wants-crypto-exchanges-corona-contingency-plans/>
- <https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disaster-recovery-plan-drp>

4.12 Evaluation

It is recommended that a crypto-asset exchange be assessed and evaluated for threats, vulnerabilities, and cybersecurity risks that are generally inherent in the traditional Information Technology (IT) environment. Others include novel threats, vulnerabilities, and cybersecurity risks exclusive to crypto-asset exchange information platforms – Crypto-asset exchange cybersecurity best practices evaluation should be based on this criteria.

Before operation commencement, the crypto-asset exchange must address and understand cybersecurity basics as it handles transactions and crypto-assets. Moreover, it should practice these cybersecurity fundamentals for many purposes: to protect the crypto-asset information system architecture against malicious cyber-attacks. More often than not, centralized crypto-asset exchanges are hacked and customer funds are stolen, and therefore lost to malicious hackers sans attendant consequences. Centralized crypto-asset exchanges providing custodial services must bear responsibility for customer crypto-asset financial data safety and security during the entire crypto-asset financial data lifecycle as long as the asset is custodied on the exchange.

The evaluation of sustainable crypto-asset exchanges is safe enough for customers based on the criteria mentioned above as the inherent factors for consideration and determination. This is evidenced in a report by the CER and Hacken professionals in a "Top 100 Crypto Exchanges According to the Cybersecurity Score (CSS)", where the criteria were made out as a comprehensive assessment model of security audits comprising of the crypto-asset exchange system essential components viz:

- Server Security
- User Security
- Ongoing Crowdsourced Security Assessment (OCSA)

As part of its cybersecurity hardening and evaluation motivation, the crypto-asset exchange should institute a bug bounty campaign crowdsourcing by inviting cybersecurity researchers and hackers to find vulnerabilities in the exchange system software code and configuration errors that might have slipped through/past the exchange developers and the entire security architecture teams.

See URLs:

- <https://www.secureworldexpo.com/industry-news/cryptocurrency-exchange-cybersecurity>
- <https://www.securitymagazine.com/articles/87925-how-to-evaluate-your-security-systems-cyber-ris>
- <https://www.securitymagazine.com/articles/87925-how-to-evaluate-your-security-systems-cyber-risk>
- <https://hacken.io/research/researches-and-investigations/top-100-crypto-exchanges-according-to-the-cer-cyber-security-score-css/>
- <https://hacken.io/wp-content/uploads/2019/07/100-Exchanges-CSS-Report.pdf>

4.13 Physical Controls

Physical controls are security measures implemented in a structured definition, used for deterrence or unauthorized access prevention to sensitive system materials. These controls may make provisions that logical, reasonable, physical, and authorized access to a critical system database infrastructure and data record alone, are permitted. The two broad access control types are either physical or logical. Physical access control applies to and limits access to physical Information Technology (IT) assets, buildings, rooms, and any physical hardware piece of property. On the other hand, logical access control addresses computer network access, connections, and system data files.

See source URL: <https://searchsecurity.techtarget.com/definition/access-control?amp=1>

Examples of relevant physical security controls are:

- Closed-circuit surveillance camera
- Motion or thermal alarm system
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- Biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods to recognize individuals)

See source URLs:







- <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-sgs-ov-controls.html#:~:text=1.2.,-1.&text=Physical%20control%20is%20the%20implementation,Motion%20or%20thermal%20alarm%20systems>
- <https://www.f5.com/labs/articles/education/what-are-security-controls#:~:text=Physical%20controls%20describe%20anything%20tangible,areas%2C%20systems%2C%20or%20assets>

It is highly recommended that crypto-asset exchange has a clear-sighted control objectives definition for crypto-asset risk assessment purposes and appropriate security controls selection. The security controls classification model comes in types: physical control, technical control, or administrative control, and by functions: detective, preventative, and corrective:



See source URL: <https://www.f5.com/labs/articles/education/what-are-security-controls#:~:text=Physical%20controls%20describe%20anything%20tangible,areas%2C%20systems%2C%20or%20assets.>

Physical controls also include crypto-asset penetration-testing, three tiers of penetration testing for more general term organizations that store, accept or transact with crypto-assets (which a crypto-asset exchange is):

Cryptocurrency Services	Network and Application Pen Testing	Social Engineering	Physical Pen Services Testing
Level A			
Level B			
Level C			

Level A

The tier-one Level A includes the network and application penetration testing phase for the exchange crypto-assets. This tier involves cybersecurity expert application software vulnerabilities exploitation; networks, systems, devices, and hosts. The penetration-testing is designed to simulate actual cyber-physical attack scenarios; create actual malicious party approach mimicking.

Level B

The tier-two Level B includes network and application penetration testing and social engineering phases. During the crypto-asset social engineering testing phase, penetration testers involve e-mail/e-mail attachments, telephone, and on-site tactics to test human asset susceptibility to a malicious attack. The social engineering penetration-testing targets including crypto-asset exchange stakeholders, employees and vendors, and attack vectors may include spearfishing, phishing, vishing, web pages, impersonation, viruses, instant messages, spoofing, malware, pop-ups, and more.

Level C

The tier-three Level C includes network and application penetration testing, social engineering, and physical penetration testing. Physical penetration testing assessment takes cognizance of physical attacks on crypto-asset facilities, crypto-asset exchange, mining rig, mining farm, hardware storage facilities, sales offices, computer devices, Bitcoin ATMs, etc. Alongside others, the three tiers jointly and severally examined how factors would fare in a crypto-asset exchange malicious cyber-attack scenario.

See source URLs:

- <https://www.redteamsecure.com/services/penetration-testing/cryptocurrency-penetration-testing/>
- <https://www.redteamsecure.com/blog/4-key-cryptocurrency-security-measures-are-you-following-them>
- <https://www.sciencedirect.com/science/article/pii/B9780124199675000089>
- <https://www.sciencedirect.com/science/article/pii/B9780124160071000133>
- <https://www.upguard.com/blog/attack-vector>

4.13.1 Facility Access

Facility access is a critical safety component that, when mentioned, people tend to think of what it means traditionally, like having a security guard sitting behind an office desk all day guarding the office building facility. This is how companies protect their facilities and employees. This facility safety procedure perception has changed over time. The facility may face industrial espionage, fire damage, and other natural disasters; even with a burglar alarm system, people with bad intentions can secure unauthorized entry through the facility doors. It is a company's responsibility to protect employees and assets from harm and losses, and this protection begins at the facility door entry-point. Access control to facilities and job-sites form a workplace safety-critical component.

Facility Access Control

A crypto-asset exchange company operator should maintain control over ingress and egress from its facilities and job-sites so that only authorized visitors, vendors, and employees are allowed; and with restrictions and limitations wherever possible. There should be an easily accessible record of visitors, vendors, and employees with ingress and egress; where they are, what they are doing, and when

they leave. In a fire or natural disaster event, the employees, vendors, and visitors' whereabouts may be accounted for to first responders. Visitor and vendor management functions may also be automated.

Apposite is a technology-based system to scan government-issued IDs such as driver's licenses, sex offender immediate check performance, criminal history registries, print temporary ID badge complete with photograph; electronic access control systems having reliance on log-in access credentials of the user, vendor, employee, visitor, access card readers, auditing and reports to track employees, vendors, and visitors. There should be a second scan that records employees, vendors and visitor's departure times. In emergencies, the company can immediately access the list of employees, vendors, and visitors within the facility.

Three access control functions recommended for crypto-asset exchanges:

- **Authentication** involves employee, visitor, vendor, user identification and verification, to ensure they are not malicious actors that constitute potential threats to the facility.
- **Authorization** involves giving permission after verification of the user, employer, vendor, visitor, etc., to have ingress into the facility.
- **Control** involves determination regarding restrictions and limitations for the individual, in respect to areas allowed access, and to what conditions those are subject, i.e., an individual may be escorted while within the facility. Control also encompasses areas such as a record-keeping system that tracks materials leaving the facility.

See source URLs:

- <https://content.boonedam.us/pillar/making-physical-security-part-of-cybersecurity-best-practices>
- <https://www.securitymagazine.com/articles/92518-the-need-for-cybersecurity-and-physical-security-convergence>
- <https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120>
- https://www.energy.gov/sites/prod/files/2018/01/f46/cyber_securing_facilities.pdf
- <https://facilityexecutive.com/2020/08/cyberattacks-cybersecurity-and-facilities-systems/amp/>
- <https://searchsecurity.techtarget.com/definition/access-control?amp=1>
- <https://www.officespacesoftware.com/blog/5-ways-facilities-managers-can-help-strengthen-cybersecurity>
- <https://safetymanagementgroup.com/facility-access-is-a-critical-component-of-safety/>

4.13.2 Workstation Use

Generally, a workstation is a specialized, high-performance, and high-scalability computer system with a single user basic design philosophy, possessing advanced graphics capabilities, large storage capacity, and a powerful microprocessor CPU – Central Processing Unit. The workstation term is also used to reference terminals without processing capacity but with a mainframe computer connection.

The workstation has more capability than a Personal Computer (PC). Still, less advancement than a mid-range computer can manage an extensive peripheral PC workstation network and manage big data processing and reporting tasks in the process. Reduced Instruction Set Computing (RISC) architecture is implemented for most workstation microprocessors. This is diametrical to what obtains in most Personal Computers (PCs), where Complex Instruction Set Computing (CISC) architecture is implemented. With the RISC architecture, there is data processing, acceleration, and streamlining trifecta. Thus, applications software run by workstations must, by necessity, include more instructions and complexity than CISC architecture applications.

Typically workstation microprocessors offer 32-bit addresses (indicative of data-processing speed) compared to the exponentially slower 16-bit systems found in most Personal Computers (PCs). Notwithstanding, it could be found that some advanced workstations implement 64-bit microprocessors having four billion times the data-addressing capability of 32-bit machines.

Workstation's inherent high-end raw processing power accommodates high-resolution or three-dimensional graphic interfaces, multi-software sophistication, and advanced abilities for intercommunication purposes with other computers.

Uses of a Workstation

The use of a workstation addresses everyday operations and activities involved while putting the workstation to work.

1. Intensive computation A typical workstation performance is higher than that of a Personal Computer (PC). It has higher CPU power, multitasking capacity, etc. The primary use of the workstation is to carry out or perform intensive computation involving science engineering tasks.

Workstations can also be used for more intensive tasks like data visualization and manipulation, 3D design, simulation, animation, mathematical plots, rendering images or video files, searching through massive databases, recalculating large spreadsheets, and manipulating them, computer-aided design drawings or involve the running of multiple large applications simultaneously.

2. Financial and business application A workstation is used in complex financial and business application scenarios, as Personal Computers (PCs) have a slower speed for running these business applications. The PC's slow speed performance is caused by the lack of sufficient processing power and memory available on the Personal Computers (PCs).

High-end workstations are used to serve attached "client" PCs networking using resident tools and applications for data access and manipulation.

See source URLs:

- <https://store.hp.com/us/en/tech-takes/top-5-uses-for-workstation-laptops>
- <https://www.britannica.com/technology/workstation>
- <https://smallbusiness.chron.com/desktop-pc-vs-workstation-47069.html>
- <https://www.constructionbusinessowner.com/technology/how-select-right-workstation-your-company>

4.13.3 Workstation Security

Though workstations and home PCs are less prone to attacks and have fewer vulnerabilities, therefore, in comparison to networks or servers, since they may contain sensitive data, attackers often target them. Without a user's knowledge, a workstation can be co-opted in a coordinated Distributed Denial of Service (DDoS) attack scenario, where the workstation is used as a slave machine. The workstation system vulnerabilities knowledge helps remove the difficulty encountered in reinstalling the operating system and recovering from data theft.

Typical crypto-asset exchange workstations should adopt the traditional workstation security evaluation criteria. The Red Hat Enterprise Linux workstation security evaluation criteria consider the following:

- **"BIOS and Boot Loader Security** Can an unauthorized user physically access the machine and boot into a single user or rescue mode without a password?
- **Password Security** How secure are the user account passwords on the machine?
- **Administrative Controls** Who has an account on the system, and how much administrative control do they have?
- **Available Network Services** What services are listening for requests from the network, and should they be running at all?
- **Personal Firewalls** What type of firewall, if any, is necessary?
- **Security-Enhanced Communication Tools** Which tools should be used to communicate between workstations and which should be avoided?"

The above are the relevant workstation security evaluation criteria questions; whether an unauthorized user can physically access the machine and boot into a single user or rescue mode without a password would depend mainly on the sensitivity of the information the workstation information system holds and machine location. The BIOS and boot loader password protection prevent unauthorized users who have physical access to the system from booting from removable media or attaining root through single-user mode.

The user account password security level determination question on the machine being a method to verify a user identity is vital for the user, workstation, and network protection. The password security system intrinsic value importance is a significant determining factor relevant to user account password security degree on the machine.

On administrative control, standard user accounts should have no administrative status degree network access. Only an authorized user should have due access. And further, only authorized services should be running on and listening for requests from the network.

The kind of personal firewall necessary to use would depend on the system security policy design considerations. Contrary to a conventional firewall that controls policy between the networks that it connects, a personal firewall, on the other hand, usually protects only the computer on which it is installed.

According to 4.7, Security-Enhanced Communication Tools, Chapter 4 of the "Workstation Security, Red Hat Enterprise Linux 4: Security Guide" (quoted above), the OpenSSH Protocol is recommended

as the most-efficient network communication enhancement tool, a tool that has high-level, public-key-cryptography-based encryption algorithm to protect information as it travels over the Internet network. As a free implementation of the SSH protocol for network communication system encryption, the OpenSSH presents safer access to a remote machine and replaces unencrypted services like telnet and rsh. Other tools though not recommended, are the Gnu Privacy Guard (GPG), a.k.a. Pretty Good Privacy (PGP), etc.

Direct Memory Access (DMA) attack

A crypto-asset exchange should defend and harden up against DMA attacks. The DMA attack is an attack relevant and should be cognizant of a crypto-asset exchange workstation operation security. A successful Direct Memory Access (DMA) attack on a crypto-asset exchange workstation could render the workstation physically vulnerable. DMA attack allows computer system attacker penetration through high-speed expansion port presence as a side-channel attack in computer security. DMA accessories and connections allow potential, direct hardware facility access to part or all of a computer system's physical memory address by bypassing all Operating System (OS) security mechanisms, including a lock screen. Further, they allow reading all computer activities, stealing data or cryptographic keys, installing or running spyware and other exploits, or modifying the computer system to enable backdoors or other malware.

While DMA has apparent benefits and legitimate uses, an attacker can equally leverage the same DMA to unleash malicious attacks through system port and secure system direct access. It is recommended that crypto-asset exchanges as a baseline security measure protect against direct memory access attacks to the workstation. Workstations like desktops, laptops, servers, cloud environments, and relevant devices become vulnerable, despite mitigation risks' availability opportunity to these attacks, which are also known collectively as Memory Lane Attacks (MLAs), enterprise hardware pieces are vulnerable.

Workstation systems must be protected against known attacks through their ports to ensure users and companies are not left open to exploits, threats, and vulnerabilities which attackers may target at the workstation. Attackers exploit the DMA feature of specific computer devices and servers that allow peripherals direct system memory access. Recommended mitigation or discovery approach that could be deployed to deal with a workstation security breach or attack situations DMA attacks, etc. are:

1. Routine Workstation Check and Maintenance

Crypto-asset exchanges should perform maintenance and routine checks on the workstation. A workstation system test of modern computer devices could reveal potential, hidden, workstation-security system potential compromise risks. These could be through the USB port critical cyber-threat entry-point or by opening the case, despite firmware maker DMA security-issue mitigation solution availability.

Research has demonstrated that DMA attacks could occasion supply-chain danger for companies in a hypothetical research attack scenario where attackers secure hands-on access to a system and cause malicious hardware implantation therein. Further, in the same research, it was found that the

wireless card of an HP laptop with a programmable development platform could modify the system RAM during booting, and therefore gaining the device control. HP, the computer hardware company, issued an updated BIOS version to fix the issue.

Historically, it has been difficult to fix attacks given the modern security features, capabilities, and protections that are being built into silicon, hardware, and chipset vendors. Another difficulty is that it takes time for different vendors to write code that enables hardware protection and configuration for system-security before delivery to the end-user. Specific programs compromise computer systems through ports to grant direct high-speed access to the system memory. These compromised ports serve purposes to drive external monitors, memory expansion, and graphics upgrades.

2. Tools Deployment by Hardware Makers to Harden Workstation Device Against Attacks

Though hardware makers can deploy tools to harden workstation devices against potential attacks, the end-goal of such constructive steps must be to achieve potentially secure system delivery to the end-users. According to an Eclipsium Report, though chip vendors, device vendors, and vendors of operating systems develop controls to defend against threats and attacks, research has shown that many devices with built-in hardware protections are still potentially vulnerable.

It's revealed in some quarters that making a system hard against autorun setting for devices plugged into or connected with the USB port takes years and significant hacks to spur action.

3. System Access Freedom Restriction

Indiscriminate physical access grant to a workstation exposes to a significant security risk. Leaving a computer device around anywhere should be discouraged, as another malicious device could be plugged into it to compromise it and thus cause damage and system malfunction.

4. Paying Attention to the Device System Firmware

The Eclipsium cited a report issued a piece of advice relevant in a crypto-asset exchange workstation security context. It concerns the fact that though identified, inherent vulnerability attacks are not new. It is recommended that crypto-asset exchanges devote attention and efforts to the firmware of the devices acquired by them. There are tools published for DMA weaknesses exploitation in systems, i.e., Frisk's PCILeech, which allows attackers to target Windows, Linux, and Mac systems.

According to Frisk, apart from removing the log-on requirement, load unsigned drivers, executing code, and spawn system shells, PCILeech possesses the capability to insert wide-ranging implants into target kernels that allow easy access to live RAM and file system through what is called "mounted drive."

See source URLs:

- [https://www.darkreading.com/vulnerabilities---threats/enterprise-hardware-still-vulnerable-to-memory-lane-attacks/d/d-id/1336921?mc=rss x drr edt aud dr x x-rss-simple](https://www.darkreading.com/vulnerabilities---threats/enterprise-hardware-still-vulnerable-to-memory-lane-attacks/d/d-id/1336921?mc=rss%20x%20drr%20edt%20aud%20dr%20x%20rss-simple)
- https://en.m.wikipedia.org/wiki/DMA_attack

- <https://zephyrnet.com/enterprise-hardware-still-vulnerable-to-memory-lane-attacks/>
- <https://eclipsium.com/2020/01/30/direct-memory-access-attacks/>
- <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/ch-wstation.html>
- [https://en.m.wikipedia.org/wiki/Personal_firewall_\(vii\)](https://en.m.wikipedia.org/wiki/Personal_firewall_(vii))<https://www.cmu.edu/iso/governance/guidelines/appropriate-use-admin-access.html>

4.13.4 Device and Media Controls

It is recommended that crypto-asset exchanges implement device-control risk mitigation measures as part of their security control program.

Device Controls

Device controls protection measures unauthorize user access to devices to minimize possible risks to business or organization infrastructure data assets, i.e., those leveraged for data storage, data transfer, etc. The relevant device controls checklist is a comprehensive list, as it contains removable devices, printers, modems, external network adapters, connection buses such as USBs, multi-functional peripherals, and the likes.

Most device control measures restrict access by the user via system access control rules. These access control rules-based restrictions are set parameters for the identification of two device control component functions. These are access grants to specified types of devices for specified types of users or groups during a time specified, and restriction rules-set on component functions such as reading and editing of files on the data storage database system.

Device Controls Benefits

Whether as a stand-alone solution, or a part of a broader data protection solution context, particular device controls benefits exist, which are highly recommended for crypto-asset exchanges to take advantage of; such as listed here below:

- Data prevention
- Theft prevention
- Media encryption
- Monitoring
- Malware protection
- Forensics

Device Controls Software Benefits

- Visibility into who is using what devices and on which endpoints.
- Device control to ensure only legitimate business use.
- Encryption of data transferred onto removable devices to prevent use and dissemination without authorization.
- Monitoring file transfers onto and off the network.
- Logging of device usage and data transfer activities on the network.

- Keeping metadata copy/file contents transferred off the network.

Crypto-asset exchanges should maintain constant protection against USB-borne malware introduction by implementing device control basic security best practice measures such as the following:

- Controlling device use on the computer ports and endpoints.
- Controlling downloadable and "openable" file types.
- Showing which files have been downloaded.
- As a best practice, inserting only trusted removal media or devices into the computer should be prioritized.
- Anti-malware/anti-virus software installation, running and updating on the computers.
- Disabling auto-features as they are already whatever programmes are installed on the media or device.
- Data deletion on media, device, and computer once there is usefulness expiration, as data redundancy can result in potential vulnerability risks.
- Data blockers and strong password use should be considered, and password rotation should be implemented as well, where there is a reasonable suspicion that they might have been compromised.

Media controls

Media protection controls pertain to information defense through diverse media types, both digital and non-digital. Standard digital media controls examples span computers, memory cards, thumb drives, external hard disk drives, Compact Discs (CDs), Digital Video Discs (DVDs) et al. The non-digital media is a paper format an ordinary business course. Media protection controls can occasion access limitation to authorized personnel while applying confidentiality labels to sensitive information and providing media destruction instructions or information removal so that such information defies any reconstruction or retrieval attempt. Media protection controls examples are:

- Media access
- Media storage
- Media transport
- Media marking
- Media sanitization, etc.

See source URLs:

- <https://digitalguardian.com/blog/what-device-control-device-control-definition>
- https://www.google.com/url?sa=t&source=web&rct=j&url=https://staysafeonline.org/blog/security-best-practices-for-removable-media-and-devices/&ved=2ahUKEwiEnbHVhdztAhWOfMAKHUAxCGwQFjAVegQIFxAB&usg=AOvVaw2M9CMNNszDhpwX7mv_9BU_s
- <https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/removable-media-controls>