12 Things About Crypto Insurance Every VARA License Applicant Needs to Know

Every firm licensed by Dubai's Virtual Assets Regulatory Authority (VARA) needs to comply with the mandatory regulatory insurance requirements.

To provide much needed clarity on this area of confusion, ACX Compliance, the leading crypto compliance services firm globally, worked with Relm Insurance MENA, a subsidiary of Relm Insurance Ltd, the largest crypto specialized insurer globally, to create this educational summary that should answer most questions that crypto firm executives may have on the topic of crypto insurance.

Whilst these answers are tailored to the Dubai VARA regulatory requirements, we believe that they can be helpful to anyone looking at buying crypto insurance globally.

What Type of Insurance Coverage is Required by VARA?

VARA regulations mandate that licensed firms hold three types of insurance:

- **PI Insurance** - Professional Indemnity (called E&O in US)
- **D&O Insurance** - Directors & Officers
- **Commercial Crime Insurance** - which must include hot wallet

Each type of insurance is described in detail below.

#1 Professional Indemnity (PI) Insurance

Professional Indemnity (PI) Insurance, also known as Errors & Omissions (E&O) in the US, covers professionals and businesses against claims for losses or damages due to alleged negligence, errors, omissions, or breaches of professional duty. Key areas covered include:

- **Negligence:** Claims from mistakes or lack of due care.
- **Errors and Omissions:** Unintentional mistakes or oversights.
- **Breach of Duty:** Failing to fulfill professional obligations.
- **Legal Defense Costs:** Expenses for defending against claims.
- **Settlements and Damages:** Court-awarded damages or settlements.
- **Defamation:** Claims of libel or slander.
- **Intellectual Property Infringement:** Unintentional copyright or trademark infringement.
- **Loss of Documents:** Costs for replacing/restoring essential documents.
- **Dishonesty:** Claims from dishonest acts by employees (coverage may vary).

⚠ What to Watch Out For:

PI insurance is a very generic term. It's like going to a restaurant and saying that you want to eat pasta. When buying crypto insurance coverage, make sure the PI coverage is relevant to your crypto firm. There are various types of PI coverage (technology, financial institutions, fintech, miscellaneous, etc.). Many insurance firms not knowledgeable about crypto may offer a generic PI insurance that is not relevant for crypto firms, as it often excludes crypto. Many crypto firms will simply go for the cheaper option and not ensure that the PI coverage they are getting is appropriate. So, make sure that your PI coverage includes crypto.

#2 Directors & Officers (D&O) Insurance

Directors & Officers (D&O) Insurance covers the personal liabilities of directors and officers for alleged wrongful acts while managing the company. Key areas covered include:

- **Management Decisions:** Claims from decisions causing financial loss.
- **Breach of Duty:** Failing to act in the company's or shareholders' best interest.
- **Mismanagement:** Poor or negligent management decisions.
- **Regulatory Actions:** Costs for regulatory investigations and actions.
- **Misrepresentation:** Misleading statements about the company's health or prospects.
- **Shareholder Suits:** Claims from shareholders due to negative impacts on investments.
- **Corporate Governance:** Failure to comply with governance requirements.
- **Legal Defense Costs:** Expenses for defending against claims.
- **Settlements and Damages:** Court-awarded damages or settlements.

⚠ What to Watch Out For:

D&O insurance is also a very generic term. The essential aspect here is to ensure that both digital assets and securities are included as most D&O coverage globally will exclude these. For a pure crypto firm, ensuring that crypto assets are included is essential. For any crypto firm involved in tokenization or security tokens, ensuring that securities are included is essential. Our experience has shown that many brokers not specialized in crypto will not understand the nuances between utility tokens and security tokens and firms may end up with inappropriate coverage.

There are also often exclusions for subsidiaries. This is important especially for firms involved in tokenization or RWA as such assets are often issued via an SPC.

Make sure to also watch out for exclusions on certain liabilities, including regulatory exclusion, crypto exclusion, and insolvency exclusion. A regulatory exclusion, for instance, will deny coverage if the crypto firm lacks the appropriate regulatory license. This is a significant issue in the crypto industry, where obtaining the relevant license, while theoretically possible, is often impractical. Therefore, it is essential to ensure that your insurance offering comprehensively covers the specific needs of your crypto business.

#3 Commercial Crime (Including Hot Wallet) Insurance

Hot Wallet Insurance, under Commercial Crime Insurance, covers digital assets in hot wallets against theft and fraud. Key areas covered include:

- **Theft by Third Parties:** Protection against theft by external parties, including hackers.
- **Employee Dishonesty:** Coverage for losses from dishonest acts by employees or insiders.
- **Social Engineering:** Protection against losses from social engineering attacks like phishing.
- **Fraudulent Transfers:** Coverage for unauthorized or fraudulent transfers of digital assets.
- **Legal Defense Costs:** Payment of legal costs for defending against claims related to covered losses.
- **Loss Investigation Costs:** Coverage for costs of investigating the loss, including forensic analysis and cybersecurity expert fees.

Given the high-risk nature of hot wallets, security measures and comprehensive insurance are essential for businesses handling significant digital assets.

⚠ What to Watch Out For:

Specific hot wallet insurance did not traditionally exist in the insurance industry until very recently for obvious reasons. Many brokers will sell you commercial crime insurance but crypto is almost certainly excluded. This is why it is essential that digital assets in a hot wallet are explicitly included.

Many traditional insurance companies only cover assets held in cold storage, explicitly excluding assets held in warm or hot wallets. Even for cold storage, their requirements can be prohibitive for many digital asset companies, demanding measures like Faraday cages around servers. Additionally, the Specie market, which traditionally covers physical vault risk, also offers some coverage for cold storage facilities. However, this coverage has high limits but is very restrictive and does not meet VARA requirements for example.

Maximizing Comprehensive Coverage for VARA Licensing

#4 Should I buy these policies separately or as a bundle?

A crypto firm may buy these policies separately or together as a bundle. For any firms applying for a VARA license, the bundle of these 3 areas of coverage is not essential but often encouraged in order to ensure that all policies are aligned and cover the mandatory requirements.

#5 What is the coverage amount that I need to buy?

There is no explicit limit in the VARA regulations. Instead, VARA will determine the coverage during the licensing process depending on the type of business and the size. Our experience shows that most applicants will start with a $1 million coverage and that is often sufficient for many crypto firms, especially start-ups.

#6 What happens if the actual damage is higher than the insured amount?

If the actual damage exceeds the insured amount, this damage will be a liability of the crypto firm. This is important as most crypto insurance policies will have relatively small limits (e.g. aggregate $1m). In the event the company does not have enough assets, this may cause litigation or even insolvency.

#6 How long does the policy last?

Generally, these policies are issued annually and must be renewed each year. Please note that the premium you pay each year will generally change as well depending on market conditions, client losses, regulatory position, client financial position, client exposure, etc.

#7 What to do when there is a claim?

Each policy will have different requirements, but they generally require contacting the broker as soon as possible. It is important to be aware of these notification requirements and notify your broker in that prescribed time. Each policy will mention explicitly what you need to do in the event of a claim. For example, many policies will require you to contact your broker in the 12 hours following a cyber event or by the end of the policy year in the event of a D&O claim.

#8 How much do such policies cost?

The crypto insurance market is very unbalanced and in favor of the insurers. There are many crypto firms and very few insurers and insurance brokers keen to offer coverage. For this reason, premiums (i.e. the amount you need to pay each year to obtain coverage) are quite high (ranging anywhere from 1 to 10% of the coverage amount. We do not believe these premium costs will go down in the short term unless there are new providers that enter the market. Please note that many providers offer a reduced premium coverage for the stage of pre-commencement of operations as the risk is lower.

#9 How good is the level of customer support?

Due to the limited number of firms, customer service levels vary significantly in the crypto insurance sector, as the market favors insurers. So you should expect gaps in the level of customer support.

However, clients can increase the chances of receiving market-leading customer support by performing due diligence on response times, ensuring a robust claims process is in place, and swiftly providing all requested documents for smoother and faster interactions.

#10 When do I need to reach out to my insurer broker?

It is highly recommended to start engaging with your insurance broker as early as possible. However, a quote from the insurer is generally only valid for 30 days thus important to obtain it before mandatory requirement starts. Sharing timelines with your broker throughout the process is essential. As getting the quote too early often leads to the insurance firm having to restart the underwriting process.

#11 What information do I need to provide to an insurance firm to obtain a relevant quote?

In our experience, the insurer will require answers to a set of questions to provide an initial quote. However, it is very likely that you will receive additional due diligence questions from the insurer. For your convenience, you can find **here** a list of preliminary questions that you may want to provide to your broker in order to get a quote.

#12 What are the insurers I can reach out to?

ACX Compliance is not an insurance broker but rather a firm specialized in crypto regulatory matters. We would be happy to provide you with a list of brokers you can contact to get a quote, including our partner for this education piece, Relm Insurance MENA. Please note that ACX Compliance is not involved in the insurance brokerage process and all insurance related discussions need to take place between the broker of your choice and your firm.

Take Action: Getting an Insurance Quote

For existing and prospective clients of ACX who are interested in speaking with an insurance broker, please complete this form and will contact you in less than 24 hours.

Connect with an Insurance Broker Now

Who are We?

Ohannes Kouyoumdjian
HEAD OF COMPLIANCE

Leading and managing compliance team for crypto VASPs licensing and supervision boasting 8 years of experience in Compliance realm

Toms Pauders
CO-FOUNDER & DIRECTOR

Extensive experience in crypto customer support and compliance, including managing large teams for Binance in different regions such as China and Malta