# Exercise week 1

**Group**: Jellis Hurtekant, Beppe Verheijden, Stephen Bombeke, Evarist Verstraete, Serafim Ciobanu, Los Elvis

# StableCoin

Tether has indeed had problems with paying withdrawals, which was influenced by multiple factors. One of the factors was the “shake” of another stable coin situation - TerraUSD. That situation flopped due to the stablecoin not being backed by something stable (as US Dollar, other flat currencies, or gold), but it used the counterweight of 2 coins - LUNA and UST. A user/client could also exchange the LUNA and UST with each other, regardless of the prices of the prices themselves. This is probably why it started to fail, as in case one coin starts to fail, then the other one, while being dependent on it - also struggles.

The Tether case was firstly influenced by the investors starting to lose confidence in the stability of the coin itself, due to the Terra-Luna case. The coin was not fully backed on (more) stable currencies, which was controversial to the statements of the company. The company stated that it was investing the money gathered from the sales (the client’s stock/invested money) to then mix the investment with the “other investments” such as bonds in private companies, US Treasury bills, etc.

Hence, the main factors that can be linked to the necessity of IT governance (or the fact why things went wrong) is the lack of transparency from the company, which is based on the company not being clear enough about how the currency is being backed and lacking a backbone to maintain the 1 USD$ price. The other factor was the risk management failure, because the company did not manage to maintain the price (as supposed for a stable coin) of 1 USD$, which led to more clients to start withdrawing funds, and hence - losing more capitalization. To fix the situation, the company should have thought of other methods of handling the investments of clients, and not trying to capitalize on more investments into other companies, as the flat currencies give more stability.

Sources:

[The shake of TerraUSD](https://www.sciencedirect.com/science/article/abs/pii/S1544612322005359)

[Tether withdrawals](https://www.theguardian.com/technology/2022/may/22/tether-pays-out-10bn-in-withdrawal-since-crypto-crash)

# Quixey

Quixey looked like a very promising application, with some interesting functionality being set as the base, however the failure of it was influenced by the cooperation between other businesses.  
According to one of the sources, the company behind Quixey needed to start a fund raiser, and considering the functionality of looking for information across all the applications on the user’s phone, it got enough investors willing to take a share. One of such companies was Alibaba, which at the very beginning managed to invest a significant amount of money and get a commercial contract.

Over the years, the funds raised were getting bigger and bigger, however Alibaba was still having the most share in the company. The cooperation between Alibaba and Quixey (and probably other companies) was not as smooth as expected, which led to the leaders questioning the software development capabilities of the company, due to functionality not getting released on time. Additionally, the company (Quixey) had to change a couple of CEOs as well, which probably led to even more issues regarding the development part. Overall, there are couple of factors that seem to have led Quixey to failure. One of such factors is the importance of development of this app, as not implementing, or over implementing features will lead to a problem concerning IT governance, such as wrong decision making upon key features. Another factor is dependency on one company (or a company having too big of share), which lead to the Quixey having to deal with other problem regarding business side of the project, and it could also be a problem due to the investor having too big of a share and word in the decisions the company makes. As a side factor it should be also mentioned that the company did not want to innovate as much as they could, hence falling behind the trends and the needs of the market.

What should the company have done is most probably have several reviews of the business case, as the business model probably did not expect the investments to take over control, and then take the company in debt. Another safety measure should have been the focus on key features and managing a smaller number of implementations, as that would be a much better governance of the app and company overall.

Sources: [The fall of Quixey](https://www.axios.com/2017/12/15/behind-the-fall-of-quixey-1513301224)

# Shyp

Shyp began as a highly promising startup, offering a service that simplified the shipping process for users. Customers only needed to take a picture of the item they wanted to ship, and Shyp would send a courier to collect, package, and ship it. The company handled all logistics, including selecting the most cost-effective shipping carrier—such as FedEx, UPS, or USPS—to complete the delivery.

The company attracted significant venture capital funding, thanks to its innovative concept. However, Shyp's business model had a critical flaw: customers were charged a flat fee of $5 per item for collection and packaging, on top of the standard shipping cost. While this seemed reasonable for larger or high-value shipments, it became problematic for customers shipping smaller, lower-value items, where the additional $5 fee felt excessive and inconvenient.

Moreover, the $5 fee wasn't enough to cover Shyp's operational costs, particularly given the resource-intensive nature of its service. Packaging, handling logistics, and paying couriers in high-cost urban markets like San Francisco quickly added up, making the flat fee unsustainable.

Compounding these issues was the fact that Shyp operated in a highly competitive industry, where shipping costs were already a sensitive point for consumers. While traditional carriers like FedEx, UPS, and USPS didn't offer the full-service packaging and logistics support that Shyp did, they provided lower-cost shipping options, making it harder for Shyp to justify its additional fees.

Ultimately, these pricing and operational challenges, along with competition in the logistics space, led to Shyp’s downfall, despite its early promise and strong funding.

# Fab

The whole situation regarding the Fab company started in 2011, when the company was represented as a dating website, however after a short time, the company decided to “requalify” as an e-commerce website and put more accent on sales and daily design inspiration. By doing this, the company quickly achieved high number of constant clients, and therefore - more clients meant more money getting gathered.

The company managed to even surpass a record set by Facebook regarding 1 million subscribers gathered within six months, and then even implemented a new method for the users to share about their new purchases.

Considering the fast growth of the company, and the nature of the service being provided, the company wanted to get a larger market share, and therefore get more users/clients to buy more items from their company. Hence, the company wanted to settle for another important market, besides the U.S. one - European market. However, the company mismanaged the funds and management and did not put enough effort to settle firmly in U.S., which led to problems with expanding towards the EU countries, as the rivalry with the newer companies/services was rising as well.

According to the source, the move to prematurely expand to Europe ultimately costed Fab over $60-$100 million dollars in capital. The expansion led to serious funding issues inside the board.

The company mismanaged most of the funds of the company, which led to most amount of money being spent on marketing, though not really helping with the attraction of newer customers, and in the nearest time, the company got surpassed by the similar service - Amazon. Subsequently, Fab was sold to PCH Innovations.

Considering the points mentioned above, it can say that the company certainly misjudged the importance of governance, such as the company decided to expand the market too early, or in an improper way. Also, the company did not consider the high costs of expansion that were a must. The better option would have been to get more clients in their initial area, and eventually start a separate campaign to settle some offices in EU for instance. The company certainly have not realized the risk of monopolization, and the risk that it can be easily surpassed due to the lose of their identity, which in this case - was the initial design.

Sources:

[The failure of Fab](https://www.failory.com/cemetery/fab)

# Sonicwall

SonicWall, once a leader in network security, has encountered significant issues in recent years that have undermined its credibility. One of the most notable challenges occurred in early 2024, when it was discovered that over 178,000 of their firewalls were vulnerable to exploitation due to a bug in their SonicOS software. This bug left a large number of firewalls publicly exploitable, raising serious questions about SonicWall's approach to security management and risk oversight (

From a governance perspective, the real failure seems to be a lack of proactive risk management. With such a large user base relying on their firewalls, SonicWall should have been more aggressive in identifying and patching vulnerabilities. Instead, the response felt too reactive, with many devices left exposed to attacks before any action was taken.

On top of that, the communication with customers left much to be desired. When security issues are found, transparency is key to maintaining trust, but SonicWall’s slow and unclear responses only exacerbated the situation. It’s one thing to face a vulnerability, but failing to properly inform and reassure users amplifies the damage.

**What could have been done differently?**

1. **Better patch management**: SonicWall should have developed a more robust system for regularly updating and securing its software. Given the size of its customer base, ensuring that vulnerabilities are addressed quickly would have prevented many of the issues they faced.
2. **Clear communication**: Instead of keeping customers in the dark, SonicWall should have been upfront and transparent about the risks posed by the vulnerability. Communicating more clearly would have helped rebuild trust with their users.
3. **Focus on legacy systems**: A lot of the compromised devices were older models still in use. SonicWall should have either provided better long-term support for these systems or more actively encouraged customers to upgrade to newer, more secure products.

**Governance Insights**:

* **Risk management failures**: This situation highlighted gaps in SonicWall’s risk management processes. Stronger governance practices could have helped identify and address these vulnerabilities before they were exploited.
* **Stakeholder communication**: Clear and timely communication is crucial in situations like these. SonicWall’s failure to keep its customers informed weakened their standing in the market.
* **Innovation and future-proofing**: SonicWall needs to be better at aligning its innovative products with long-term strategic goals to stay ahead of security threats.

Sources:

[Bishop Fox](https://bishopfox.com/blog/its-2024-and-over-178-000-sonicwall-firewalls-are-publicly-exploitable)

[Security Affairs](https://securityaffairs.com/168112/hacking/sonicwall-sonicos-bug-exploited.html)