

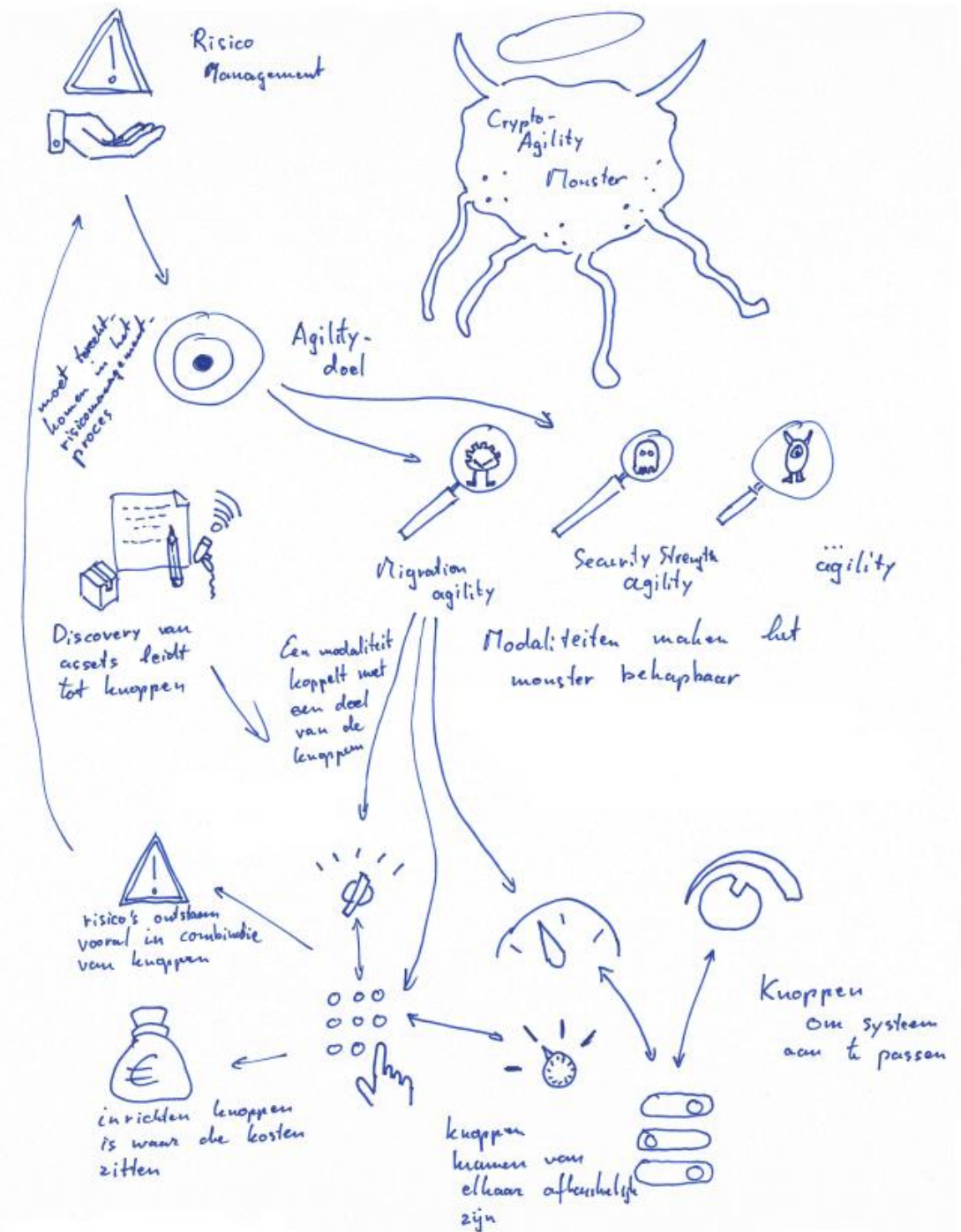
Het crypto-agility monster

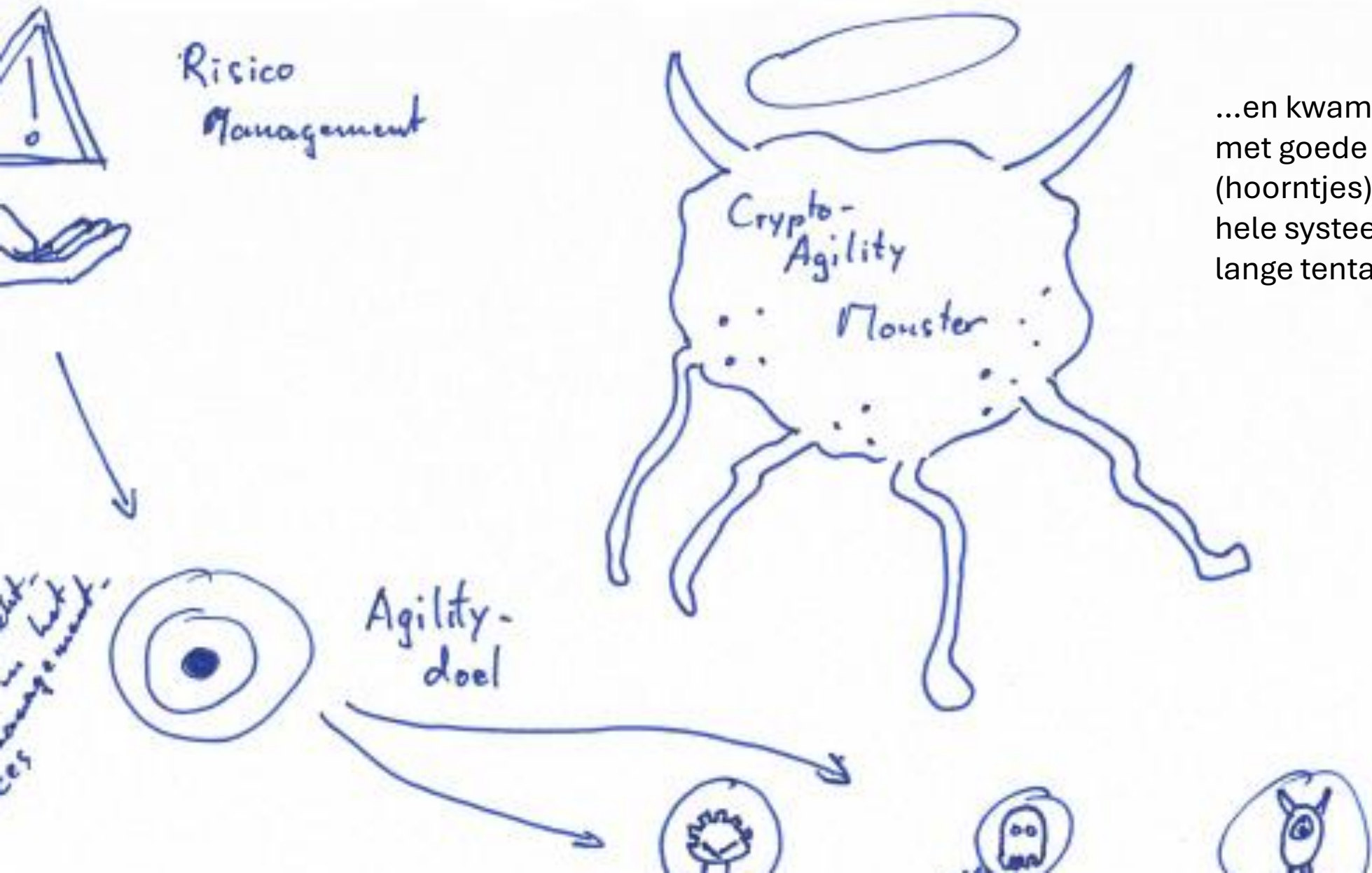
Dion Koeze – onderzoeker NCSC
(Robert Seepers – adviseur NCSC)

[Het crypto-agilitymonster op een bierviltje | Expertblogs |
Nationaal Cyber Security Centrum \(ncsc.nl\)](#)

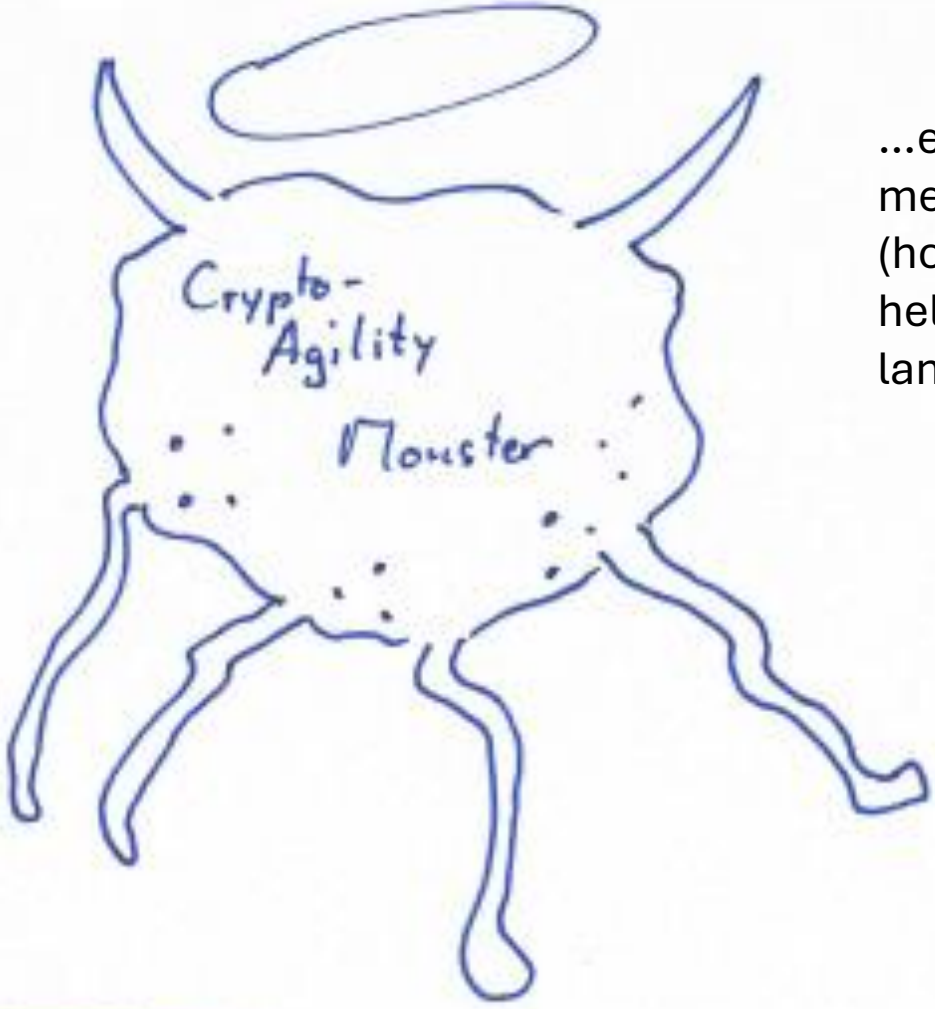
Agile zijn met cryptografie, klinkt logisch... maar hoe dan?

Na het stellen van deze vraag zijn de NCSC'ers op onderzoek uitgegaan...





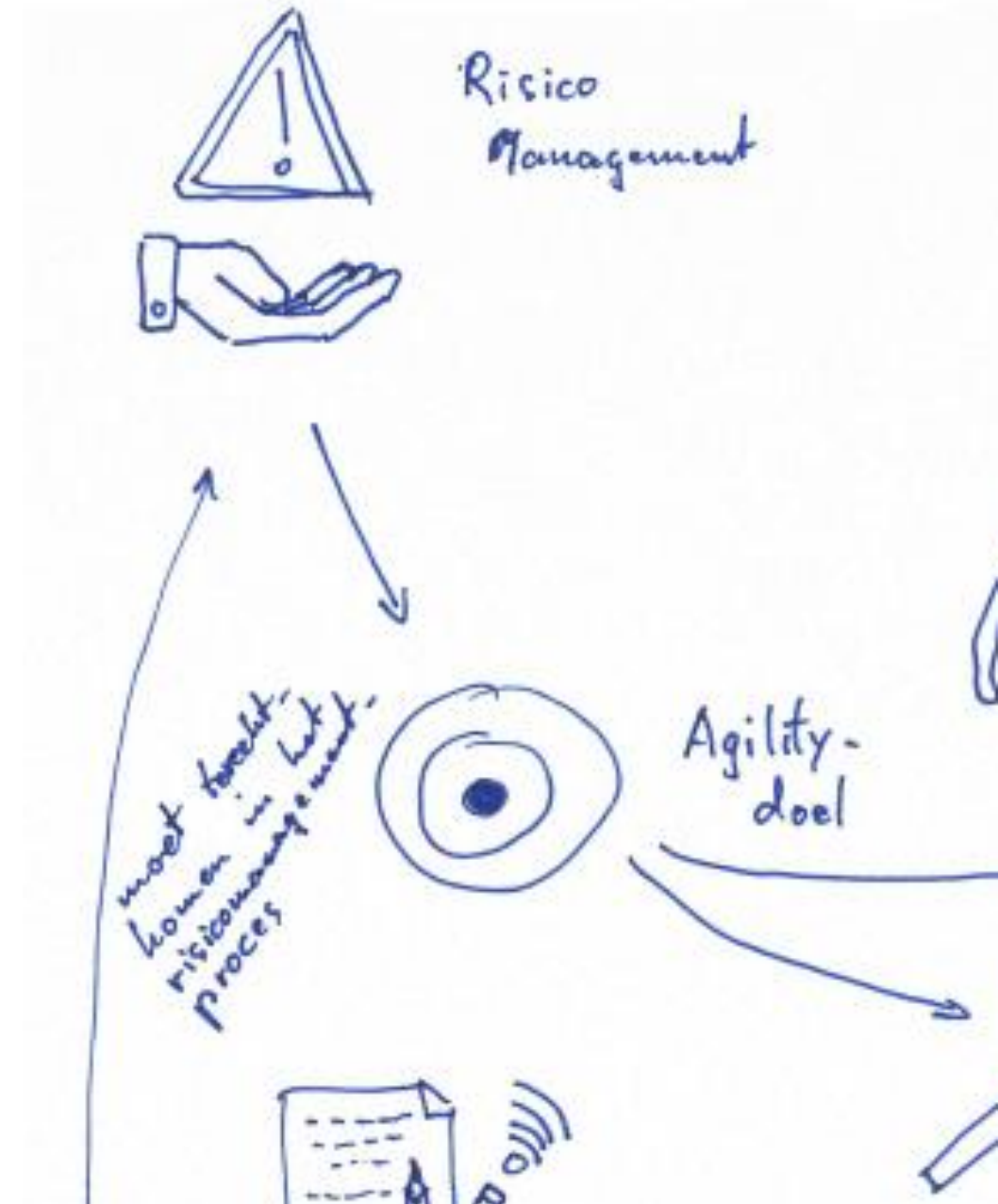
Risico Management

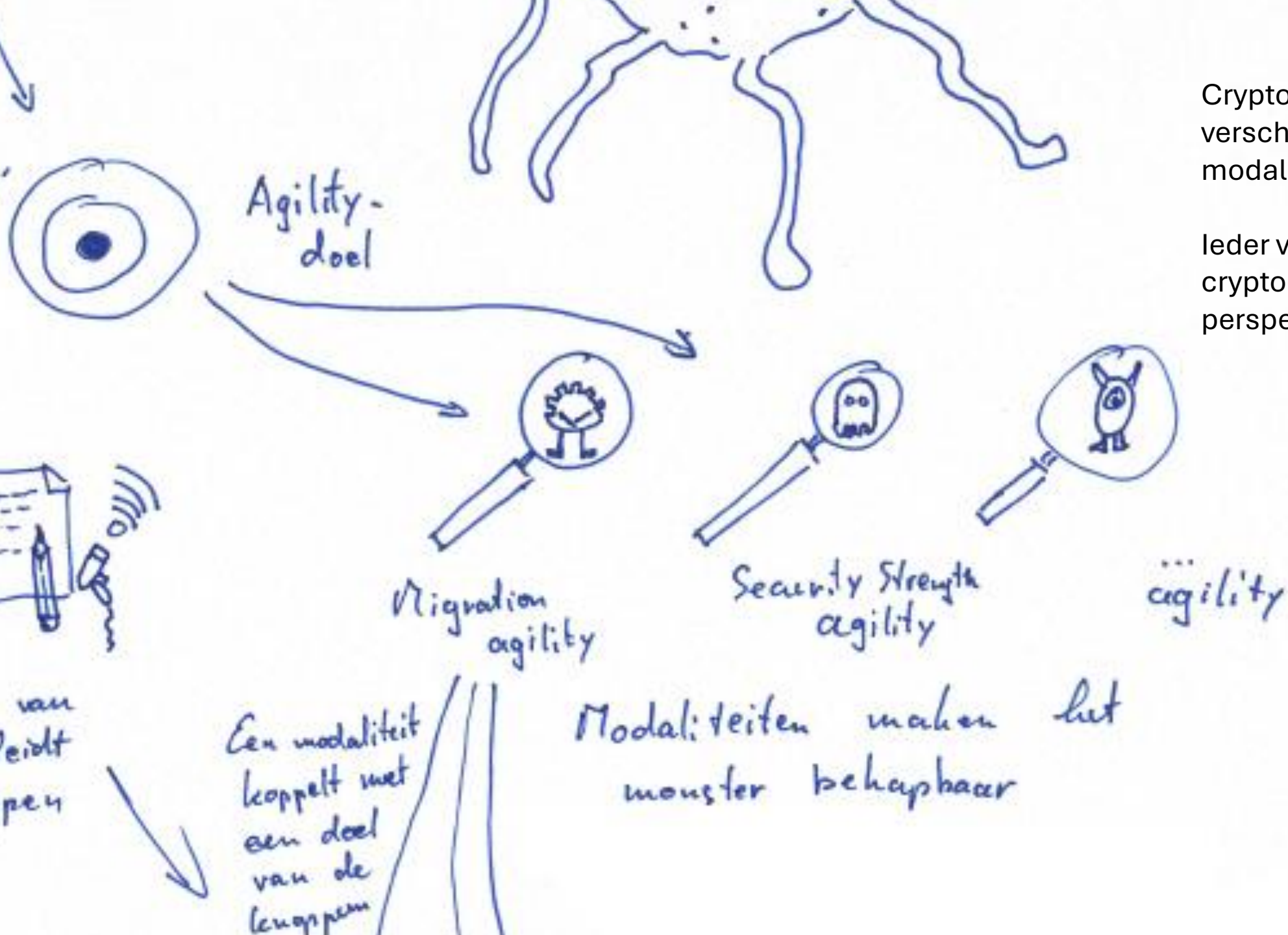


...en kwamen een monster tegen met goede (aureool) en kwade (hoorntjes) kanten dat zich door het hele systeem verspreidt met zijn lange tentakels.

Als we terug naar de basis gaan is agility een mogelijke maatregel ingegeven door risicomanagement.

In dit geval het risicomanagement van de PQC migratie.





Crypto-agility heeft verschillende verschijningsvormen, of modaliteiten.

Ieder van die vormen bekijkt crypto-agility vanuit een ander perspectief.



oudstaan
in combinatie
knoppen

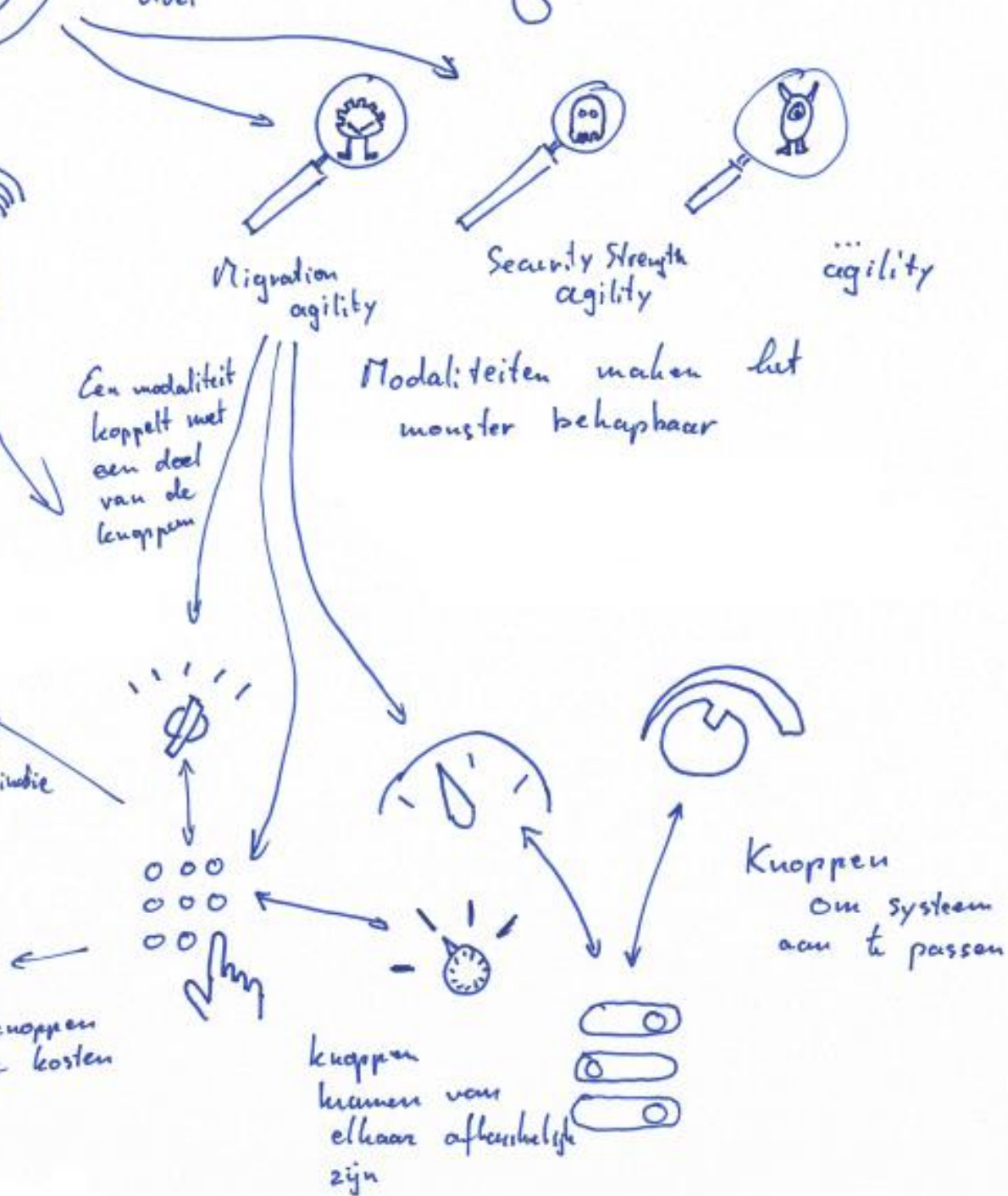
den knoppen
aar de kosten

Knoppen
Om systeem
aan te passen

knoppen
kunnen van
elkaar afhankelijk
zijn

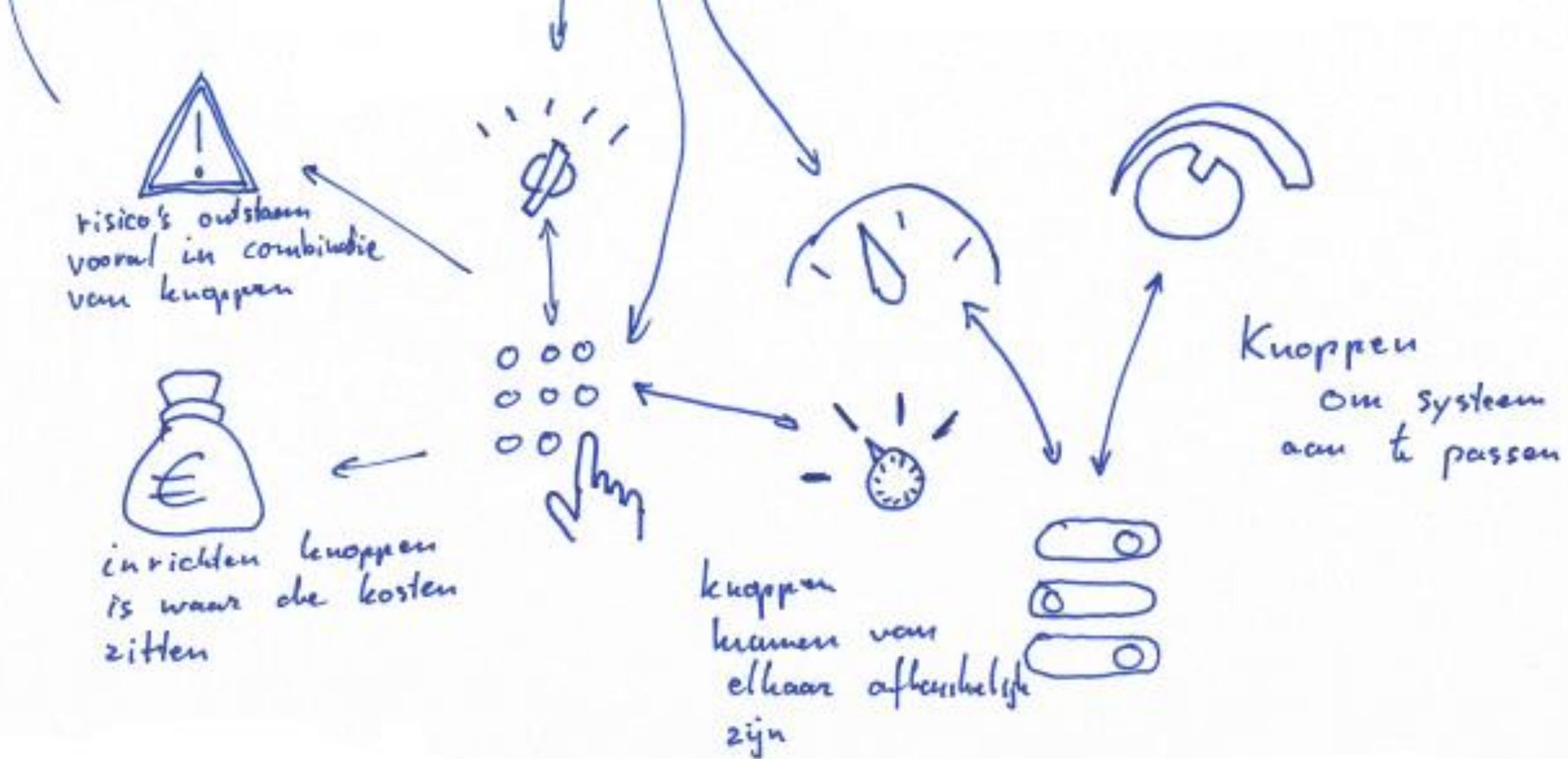
Ieder systeem heeft 'knoppen'
waaraan gedraaid kan worden.

Sommige knoppen zijn niet zo
agile, gaan erg stroef of
ontbreken, andere zijn goed
geolied.



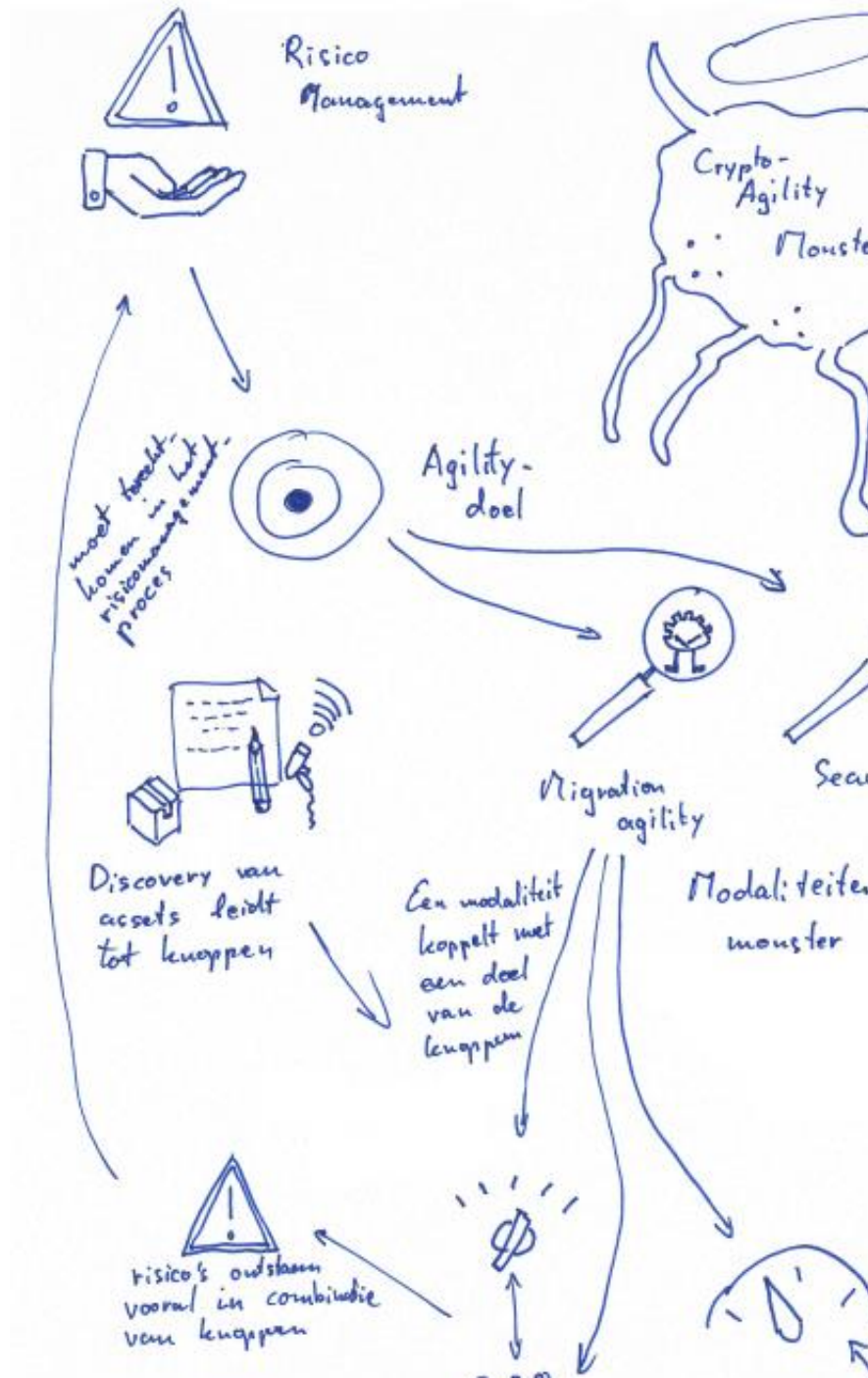
Door te bepalen welke knoppen koppelen met een modaliteit die je nodig hebt om het agility-doel te bewerkstelligen, krijg je inzicht in hoe de inrichting en instellingen van een systeem bijdragen aan crypto-agility.

Of ook wat er nog voor nodig is om dit voor elkaar te krijgen.



Vanuit de knoppen moet de koppeling worden gemaakt met kosten, nieuwe risico's en mogelijke andere effecten.

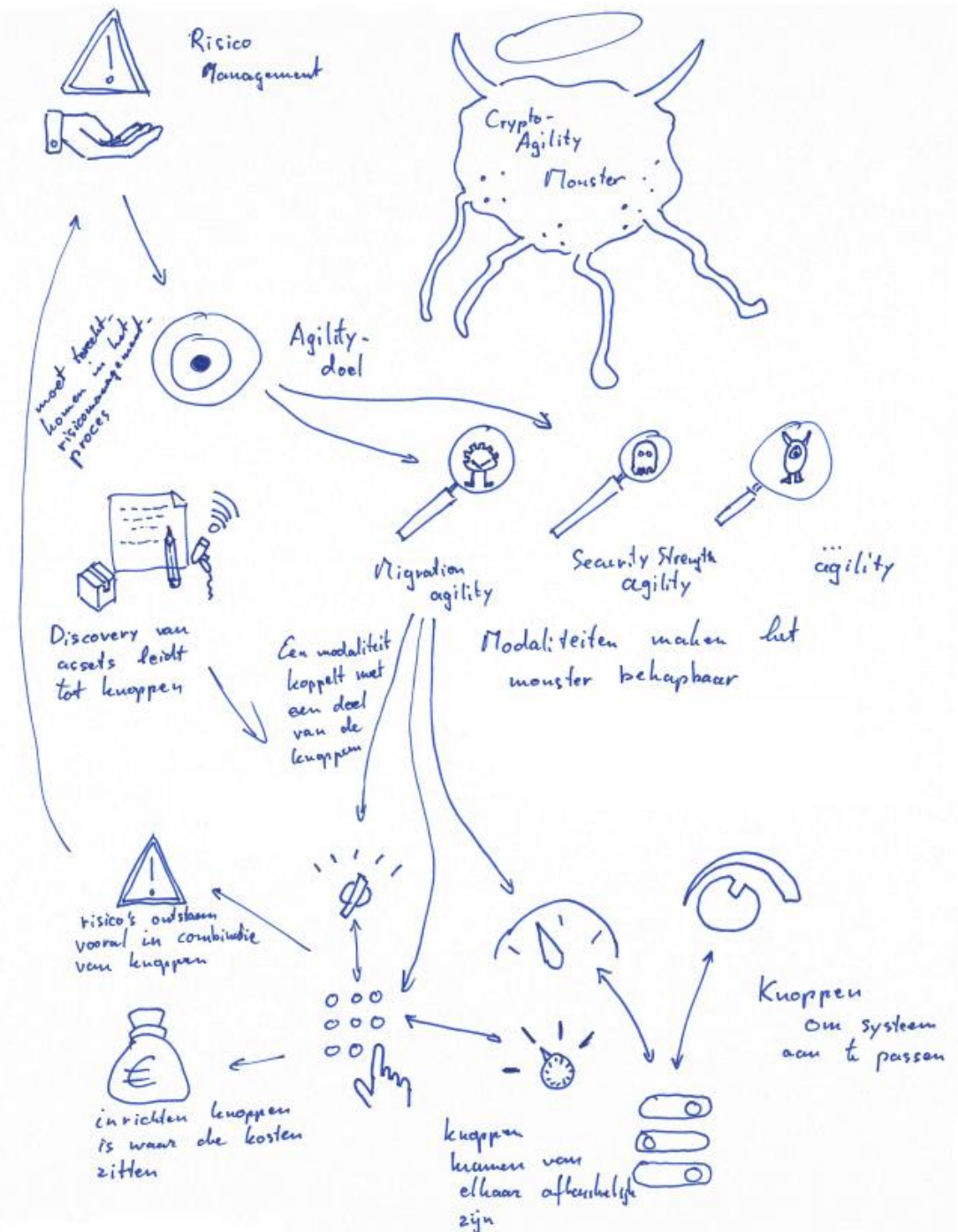
Deze nieuwe risico's moeten weer meegenomen worden in het risicomanagement.



- ~15 min: Schrijf je opmerking op de juiste kleur en plak hem op de juiste plek
- ~15 min: Bepaal de meest waardevolle opmerking met je groep (je mag opmerkingen samenvoegen of nieuwe toevoegen)

Kleur briefjes	Vraag / onderwerp
Groen	Wat zijn de sterke punten? Wat geef je nieuw inzicht?
Rood	Welke knelpunten zie je in dit model?
Blauw	Wat is nog een open plek? Wat is nog onduidelijk?
Geel	Hoe heeft architectuur invloed op dit model? Is dit model congruent met de NORA architectuurprincipes?

- In groepen
 - 1 groep online op Miro: link
 - 3 fysiek op locatie met post-its
 - Iedere groep heeft een begeleider
 - Begeleiders van groepen op locatie vullen Miro
- Straks: ~15 minuten terugkoppeling
 - Licht de meest waardevolle opmerking van iedere kleur toe



- Terugkoppeling
 - Licht de meest waardevolle opmerking per kleur toe aan de groep.
- Wil je dit verder uitdiepen?
 - [Het crypto-agilitymonster op een bierviltje | Expertblogs | Nationaal Cyber Security Centrum \(ncsc.nl\)](#)
 - NCSC is voornemens een handreiking te schrijven en zoekt daarvoor input en reviewers
 - Spreek ons aan of stuur een email:

Dion.Koeze@ncsc.nl

