Trust: the unloved sibling

Piotr Cofta

http://trust-governance.com

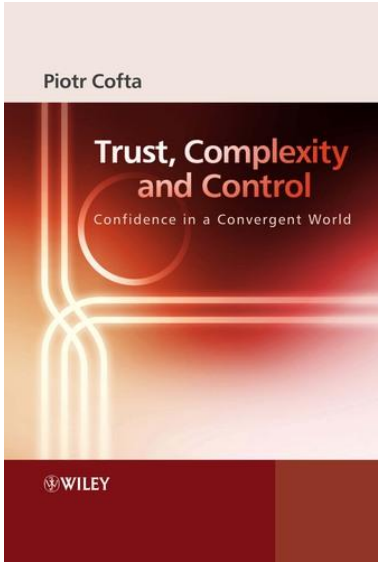
Piotr Cofta PhD CISSP SIEEE

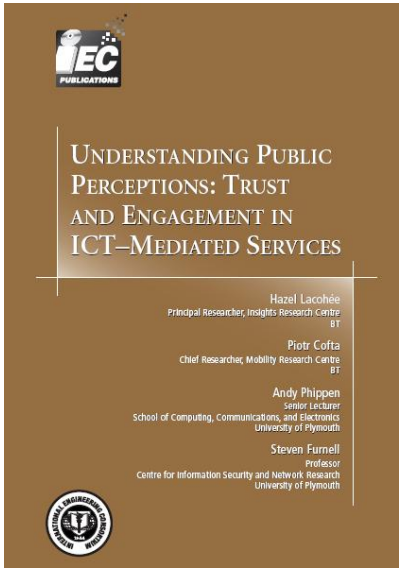
CTO Trusted Renewables

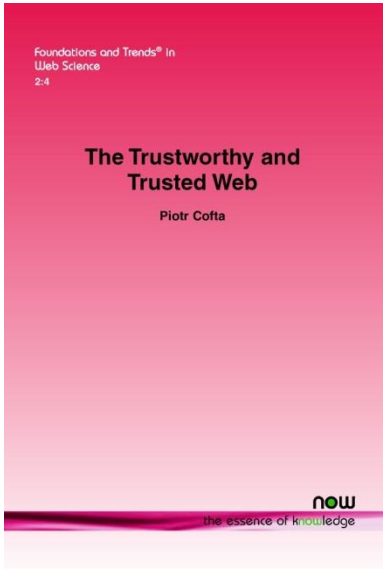
Risk and Trust

http://trust-governance.com

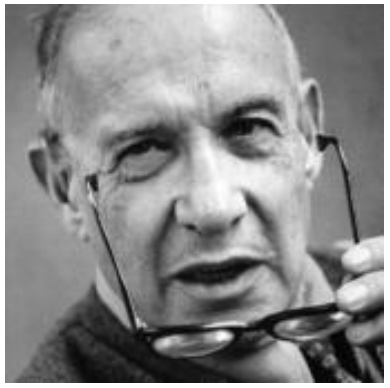
http://piotr.cofta.net



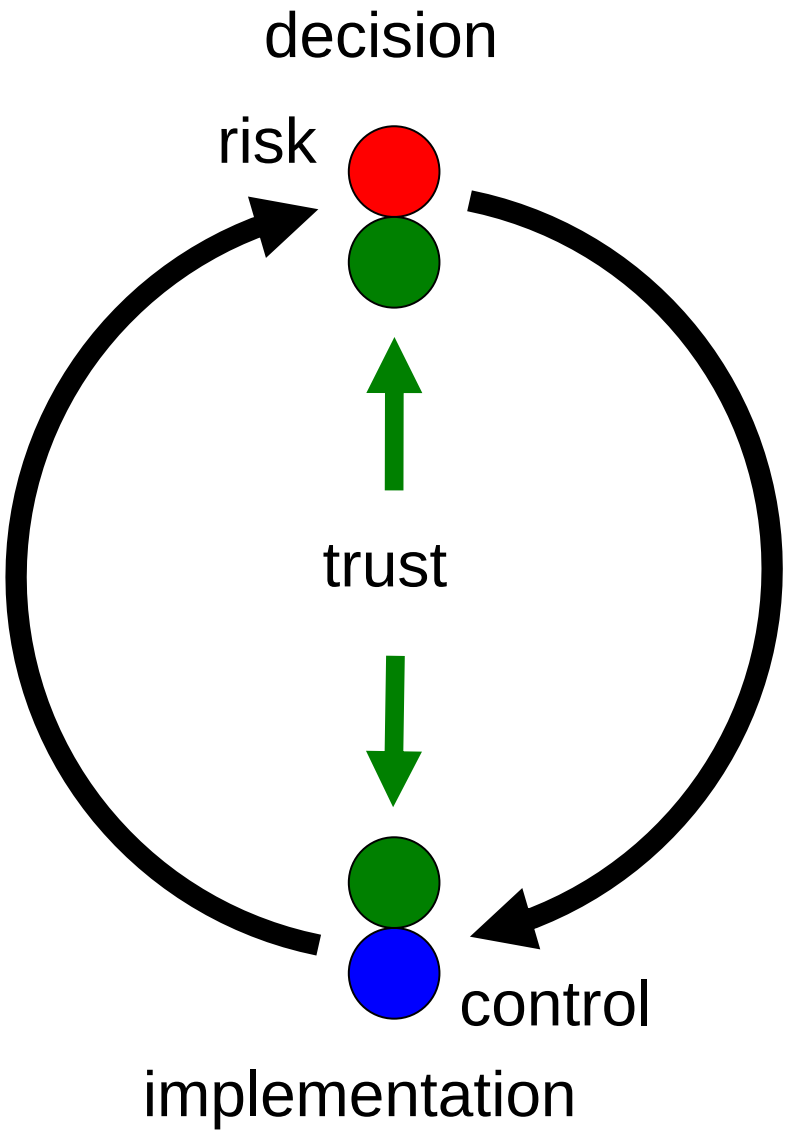




The unloved sibling..



Peter Drucker
1909-2005



All that started with a dead guy

Thomas Bayes, 1701-1761, London

Probability of future events
can be estimated
on the basis of past events.

Disclaimer

Past performance
is no guarantee
of future performance.

Ceteris Paribus*

*** "assuming everything else is equal"**

environment is assumed to be stable
not subject to whims of others
not affected by the decision itself

Corporate decisions

variable environment

INTENTIONALITY

butterfly effect chaos theory

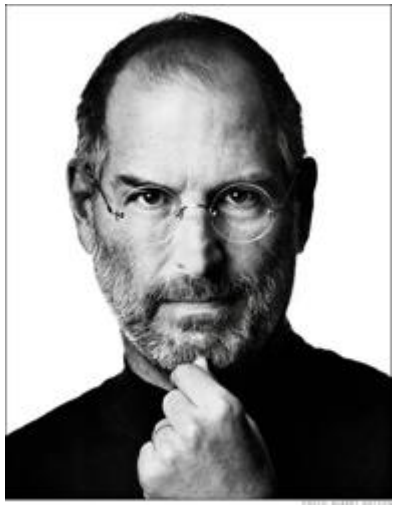
MTBF MTTF MTTR

ALE SLE

statistics actuary derivatives

stable environment

Intentionality

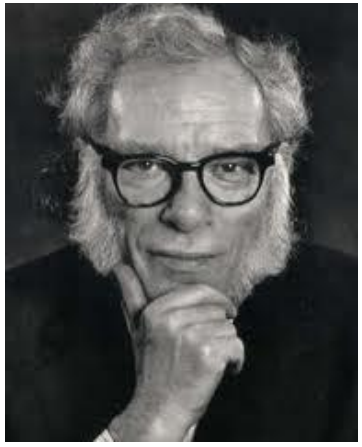


Steve Jobs
1955-2011

Environment of our decisions increasingly depends on **intentional actions** of others (individuals or organisations)

- product -> service
- hardware -> managed platform
- software -> contract
- disk -> cloud storage
- ownership -> license to use

New challenge



Isaac Asimov
1920-1992

To make good security decisions, we have to predict behaviour of **specific intentional** actors

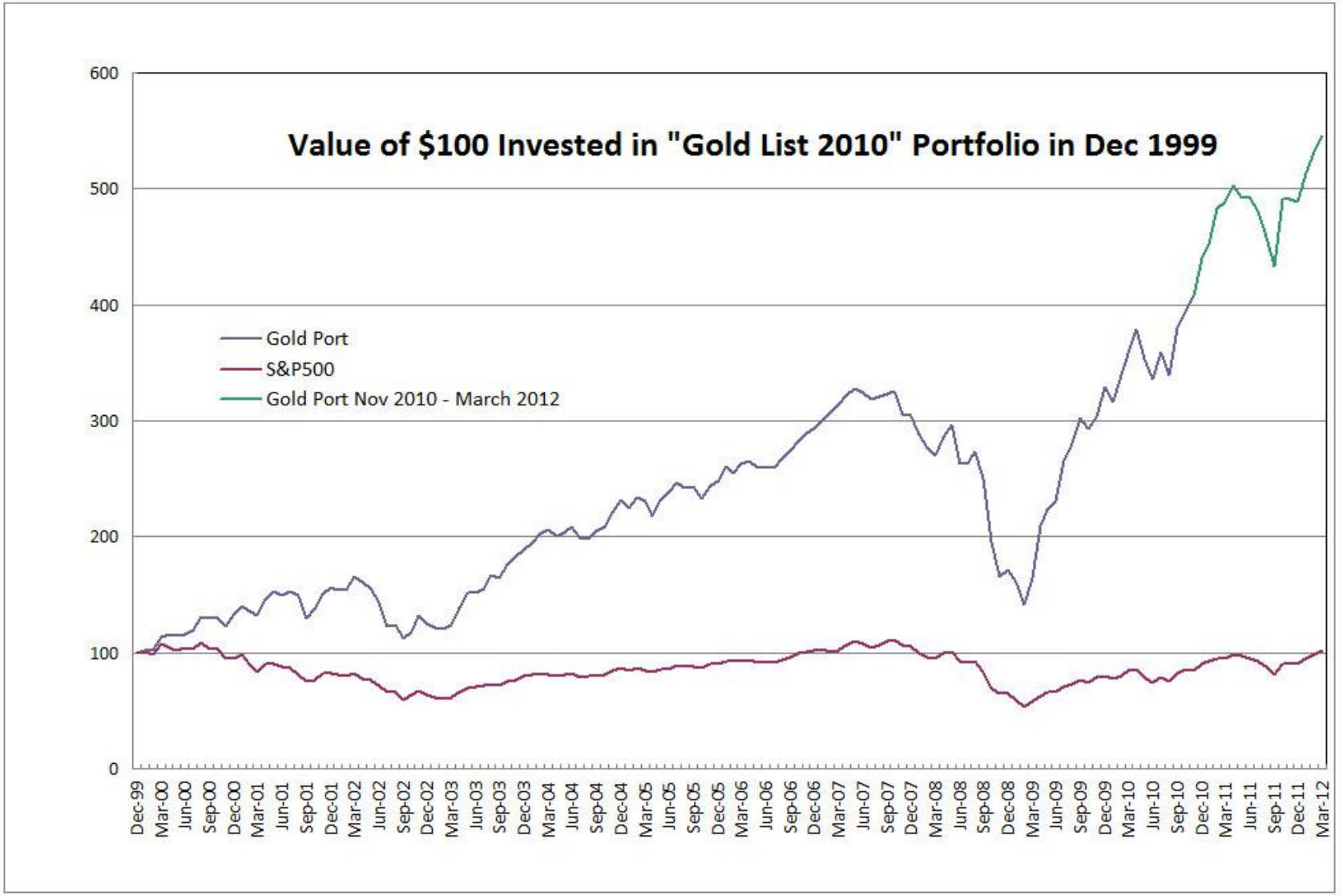
- powerful attackers
- high-level insiders
- system administrators
- contractors and collaborators
- companies and governments
- user groups

Trust

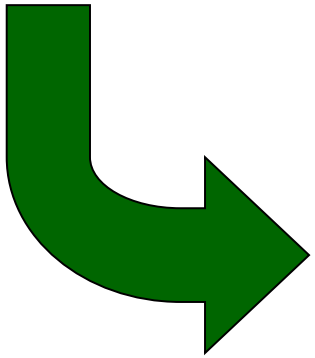
provides better prediction of intentional behaviour than risk

It is also more profitable to use trust!!

trustacrossamerica.com



Trust governance



Is he/she/it trustworthy?

What makes him trustworthy?

Can I develop trust with him?

How can I trust?

What can I do with trust?

What is trust?

But but but ..

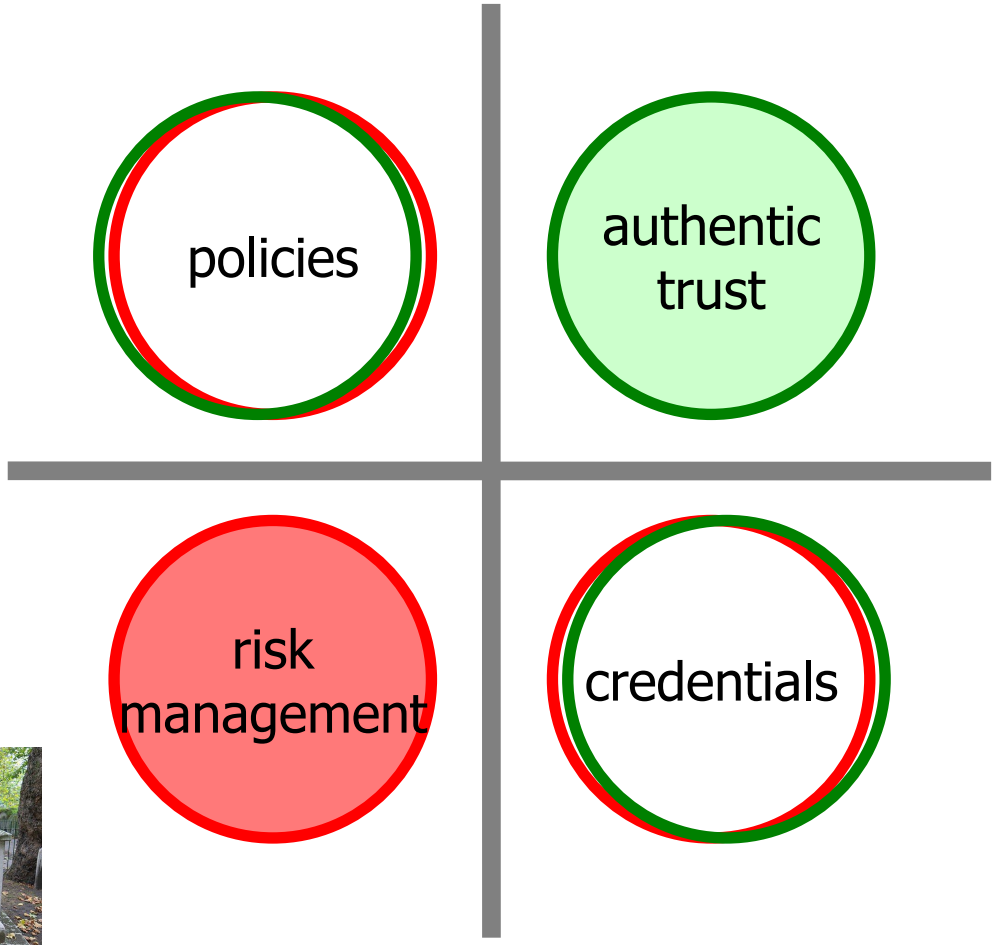
- Trust is not always applicable
- There is no definition
- Risk is here to stay
- We are not trained in trust
- We cannot measure trust

Keira Knightley
"Love Actually"

But .. trust is not always applicable

variable environment

defensive:
protecting
assets
(CISO)



offensive:
developing
opportunities
(CEO)

stable environment

But .. there is no definition

Is a new opportunity a risk?

(ISO 27001)
likelihood * impact of undesired events

only if likelihood and impact can be estimated

(PRINCE2)
events that have effect on objectives

definitely yes

(NIST 800-30)
negative impact of the exercise of a vulnerability

no, as there was no vulnerability

Trust is ..

- ... the willingness of a party (trustor) to be vulnerable to the actions of another party (trustee) based on the expectation that the other party will perform a particular action important to the trustor, irrespective of their ability to monitor or control that other party.

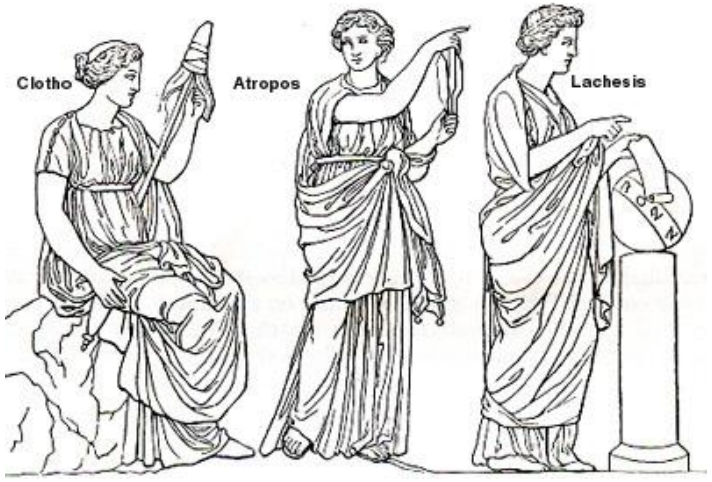
BORING

- **... the acknowledgement of trustworthiness**

But .. risk is here to stay

"It is difficult to make predictions, especially about the future"

Niels Bohr (and many others)

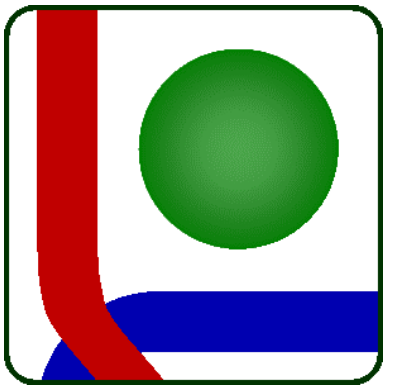


- fate (antiquity)
- destiny (renaissance)
- progress (industrialisation)
- risk (modernity)
- trust (coming)

But .. we are not trained in trust

- Ask me
- Work with us
- Check the web site:

  http://trust-governance.com
- Contribute, share, discuss
- Learn and experiment
- Build authentic trust
- Ignore 'trust gurus'

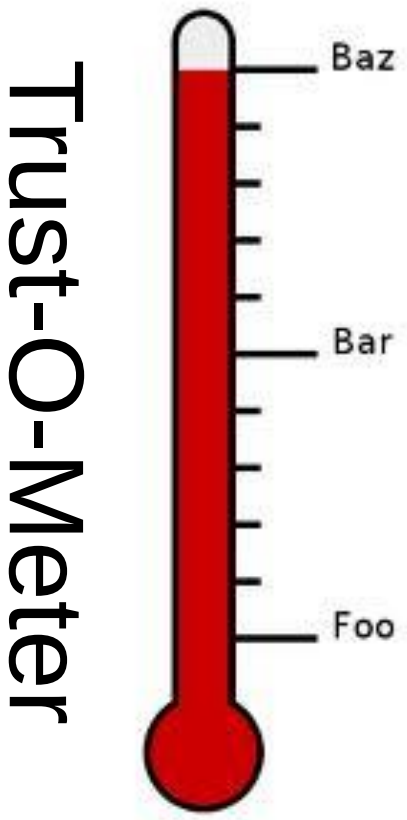


But .. we cannot measure trust

Risk used to be immeasurable

risk = likelihood * impact

Become a '10 minute expert'



- How to become an expert in trust measurement in 10 minutes?
- Use Trust-O-Meter!
  - not a tool to 'measure' trust
  - tool to reflect on trust
  - to share what you think of trust

Classical triad

- A: Competence -> [0..1]
  - He is **able** to help me, he is a professional

B: Benevolence -> [0..2]

- He seems to be a good man, he **will not** leave me alone

C: Continuity -> [0..3]

- He is really committed, his **future** career is at stake

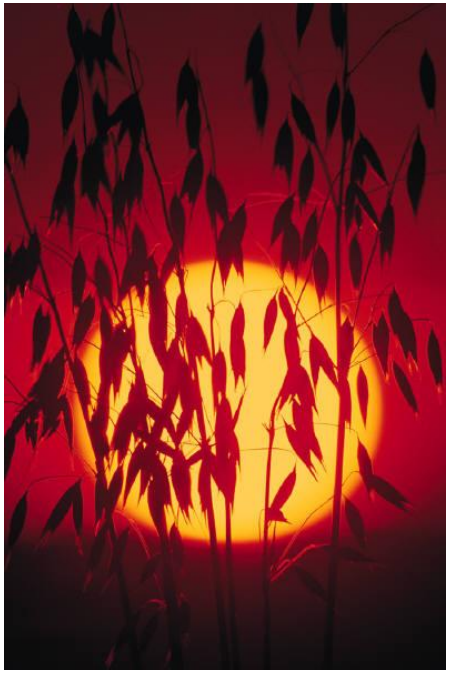
X = MAX (A, B, C)

Sharing triad

- D: Shared **background** -> [0..1]
  - We are from the same school so I understand him
- E: Shared **benefits** -> [0..2]
  - He is as much dependent on me as I am on him
- F: Shared **values** -> [0..3]
  - We both observe the same fundamental values

Y = MAX (D, E, F)

Social triad



- G: Familiarity -> [0..1]
  - The situation and the type looks familiar and it turned out to be good
- H: Stereotyping -> [0..2]
  - Doctors are trustworthy, and he is a doctor
- I: Similarity -> [0..3]
  - He is like myself, or like a person I found trustworthy

Z = MAX (G, H, I)

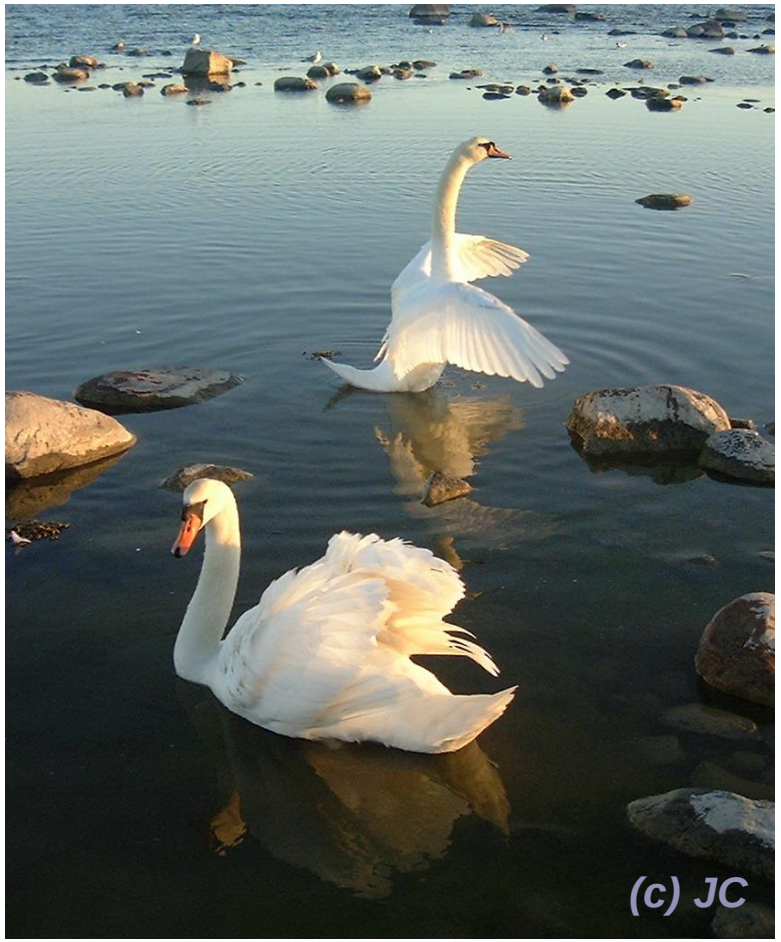
Results

X + Y + Z -> [0..9]

- 0-1: Walk away.
- 2-3: Proceed with caution.
- 4-6: Try to learn more.
- 7-8: Trust, but verify.
- 9: Too good to be true.

Now, the real question

Is this what you call trust?



Thank you

Piotr Cofta

share your thoughts

http://trust-governance.com