AppSec Research 2013

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

HAUFE.Gruppe
INTERNAL AUDIT

Dr. Amir Alsbih

Chief Information Security Officer

CISSP-ISSMP

GCFA

E-Mail: **amir.alsbih@haufe-lexware.com**

Twitter: **@checkm4te**

OWASP
The Open Web Application Security Project

Technical Due Diligence?

a kind of definition...

OWASP
The Open Web Application Security Project

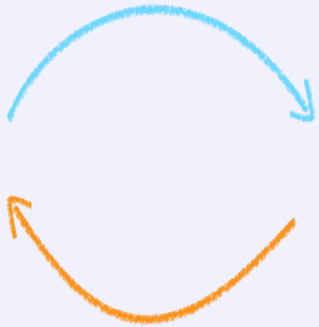
“"Due diligence" is a term used for a number of concepts, involving either an investigation of a business or person prior to signing a contract, or an act with a certain standard of care.“

~Wikipedia

it is about...

OWASP
The Open Web Application Security Project

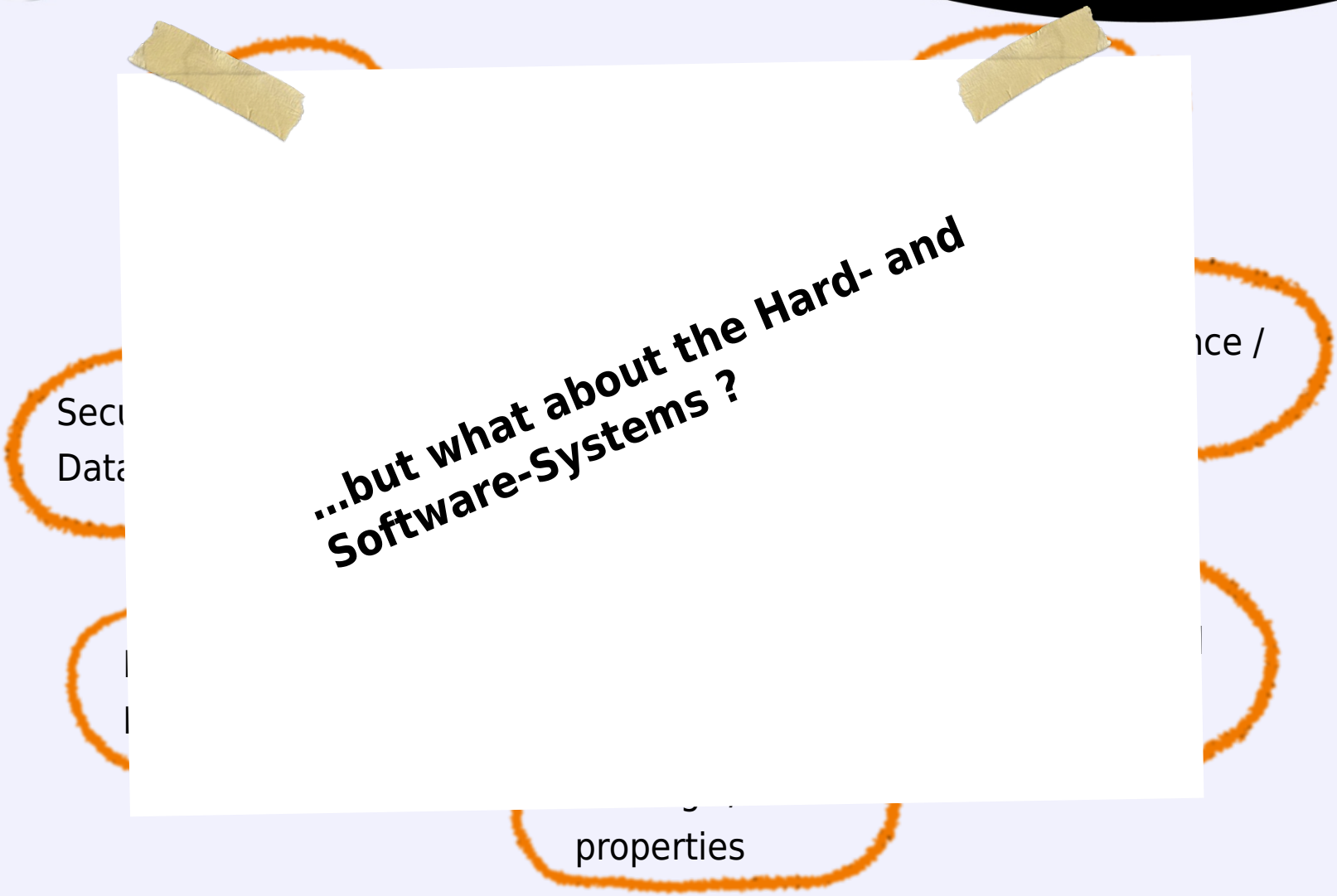
- A process to get a 360° sight on a company.
- Determination of strengths and weaknesses
- The basement for a further trustfully cooperation



- No tortures in form of endless checklists and question forms
- No stress test for the management
- No measurement of strengths or intelligence
- No delay strategy to get a better offer

more detailed...

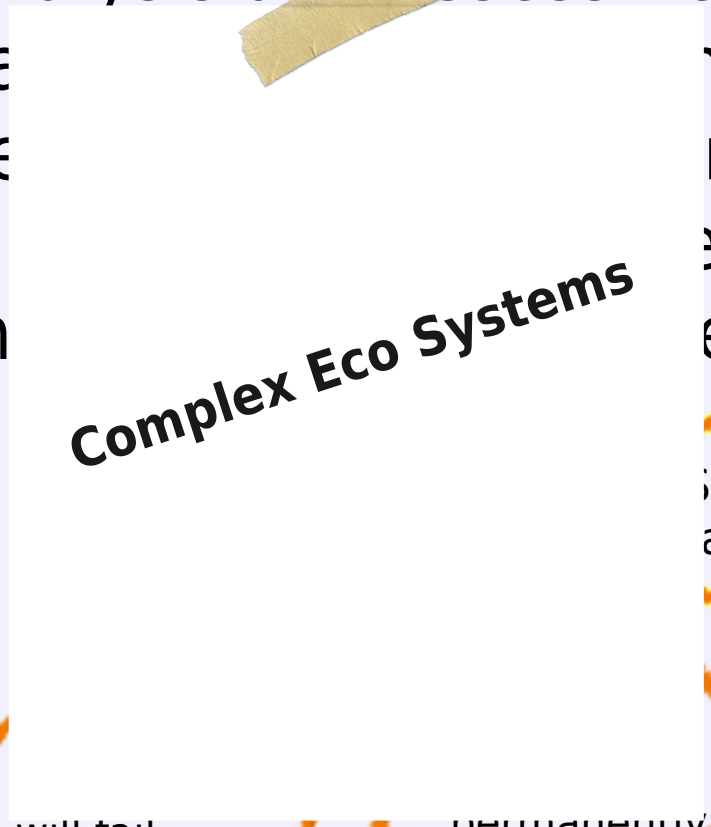
OWASP
The Open Web Application Security Project



...but think about

OWASP
The Open Web Application Security Project

Analysis and assessment of the software and
ha hould b
be nce pro
In ects the
th e comp



oftware is n
angible

will fail

permanently

No
wit
hardware

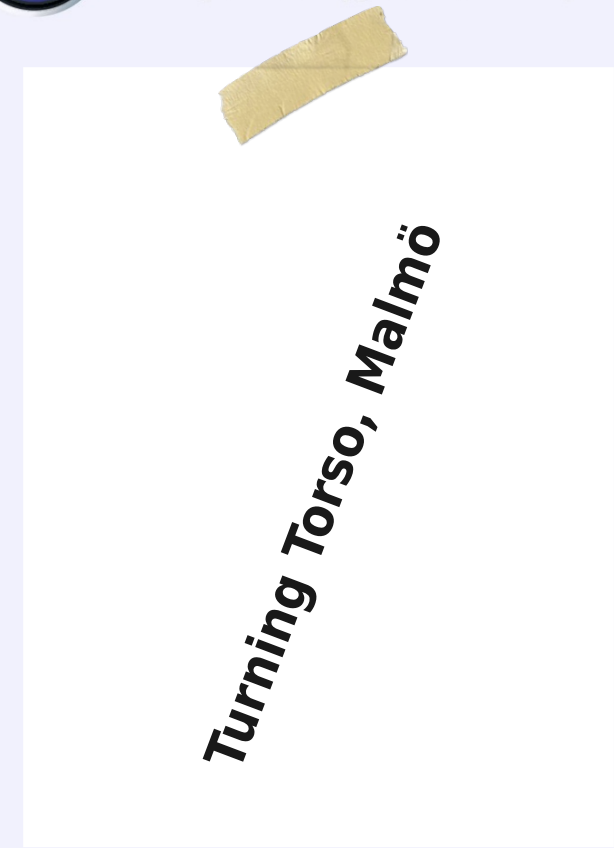
allways has
errors

OWASP
The Open Web Application Security Project

so what is the story?

the challenge...

OWASP
The Open Web Application Security Project



Please tell the weight of this building based on the image

... To difficult?

Then please tell the height of the building (tolerance <1%)

OWASP
The Open Web Application Security Project

so what is our job?

the goals are...

OWASP
The Open Web Application Security Project

Complexity

Processes

Scalability & Reliability

Maintainability

Information Security

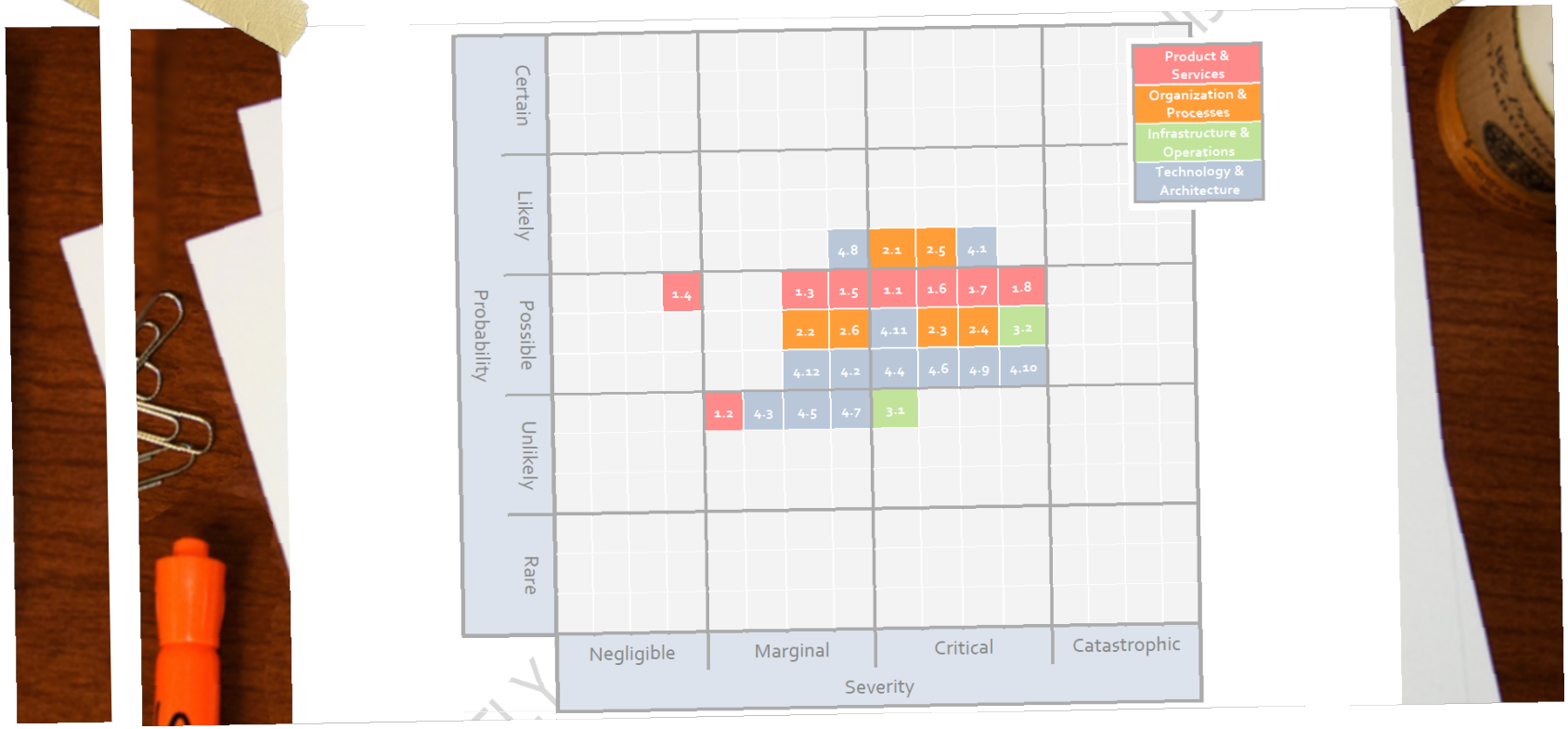
Know-How & Skills

Third-Party

Integration & Openness

a view from 30.000 feet...

OWASP
The Open Web Application Security Project



Sample Report

OWASP
The Open Web Application Security Project

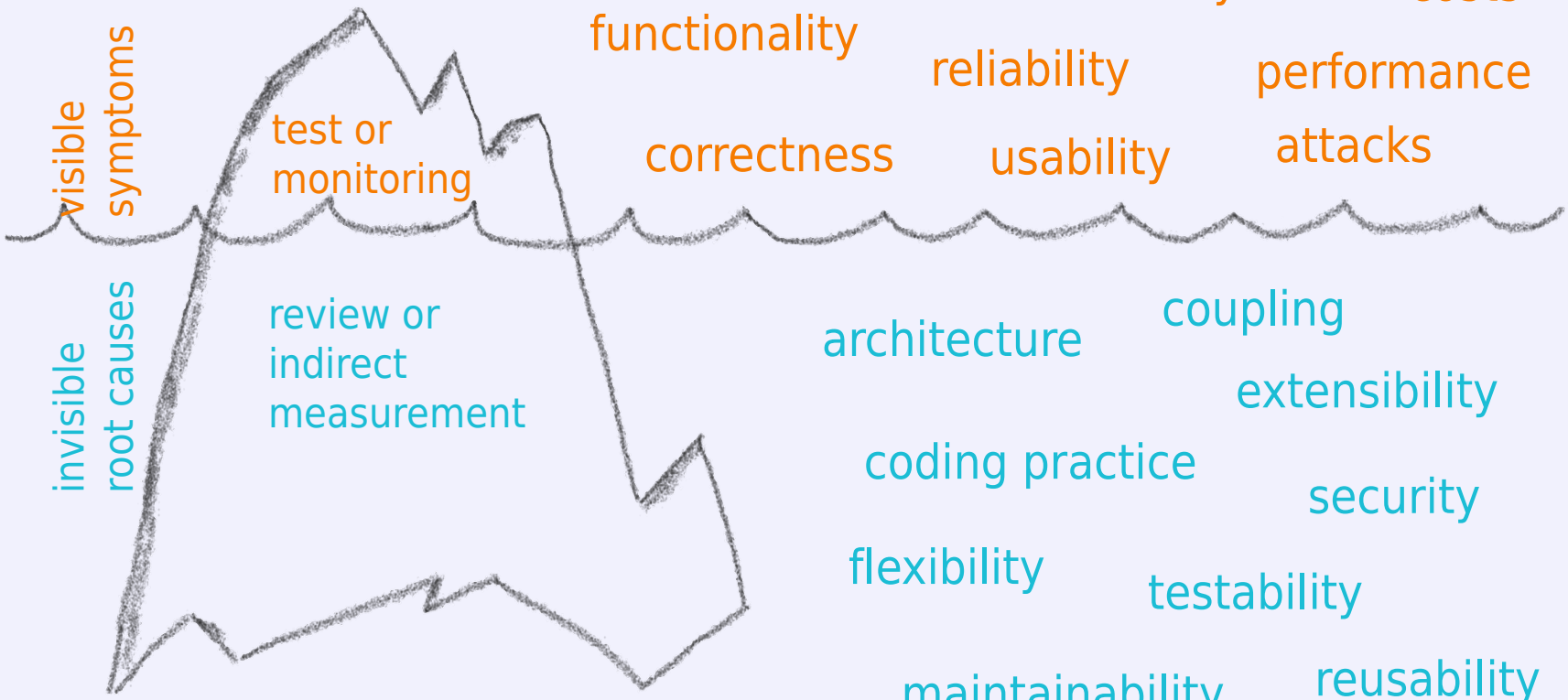
how do we get there?

Quality attributes....

OWASP
The Open Web Application Security Project

Usage	Development	Operations	Security
Usability	Manageability	Performance	Attacks
Localization	Maintainability	Reliability	Privacy
Accessibility	Supportability	Availability	Misuse
Personalization	Extensibility	Scalability	Legislation
Customizability	Flexibility		

how to measure?

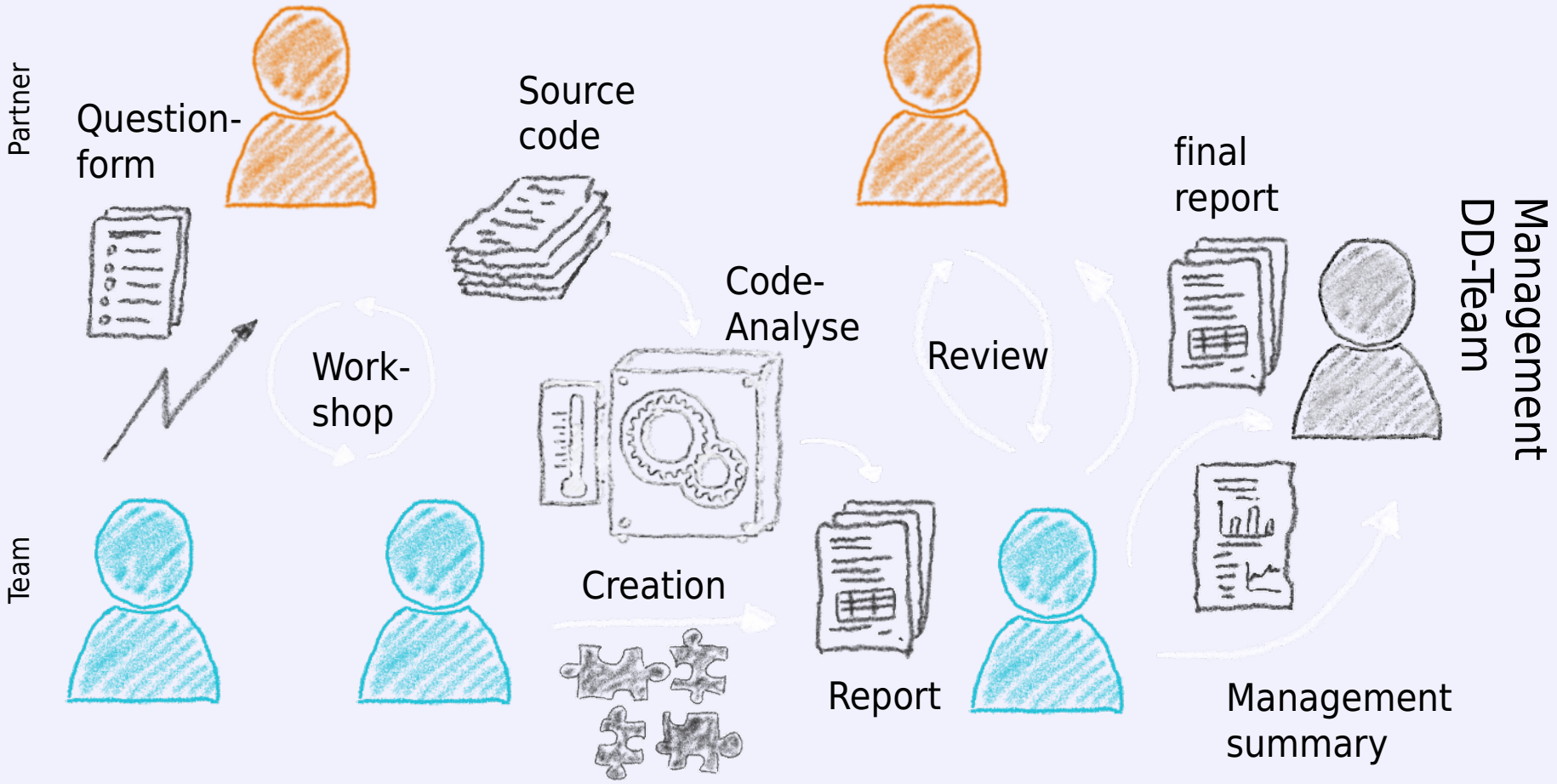


scalability
costs
functionality
reliability
performance
correctness
usability
attacks

coupling
architecture
extensibility
coding practice
security
flexibility
testability
maintainability
reusability
openness
legislation
complexity

our current approach…

OWASP
The Open Web Application Security Project



OWASP
The Open Web Application Security Project

Software Architecture

Software Architecture

OWASP
The Open Web Application Security Project

"The software architecture of a program or computing system is the structure or structures of the system, which comprise software elements, the externally visible properties of those elements, and the relationships among them."

~ **Bass, Clements and Kazman**

good software architecture

OWASP
The Open Web Application Security Project

Reliability

Performance

Security

Functionality

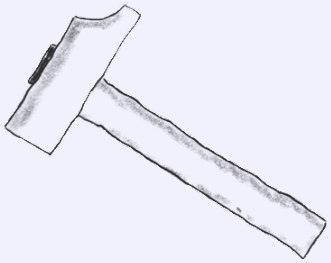
Usability

OWASP
The Open Web Application Security Project

there are no ugly babies!

have you seen this before?

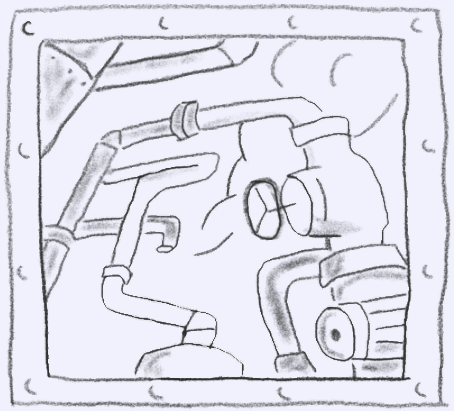
OWASP
The Open Web Application Security Project



Golden Hammer

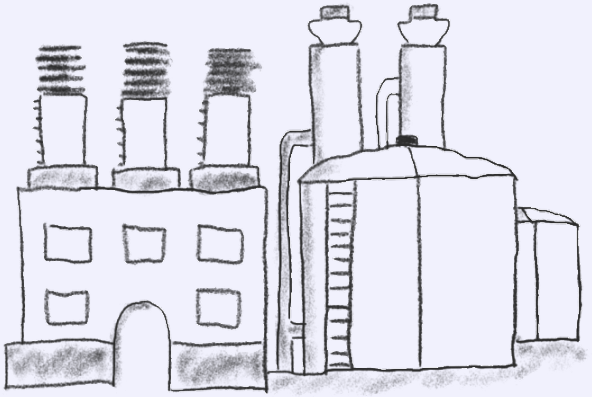
Lava Flow

Wheel Factory



Stove Pipes

Internal Platform



Gas Factory

OWASP
The Open Web Application Security Project

no easy going...

real world constraints...

Confidentiality

Documentation

Expert Knowledge

Time Frame

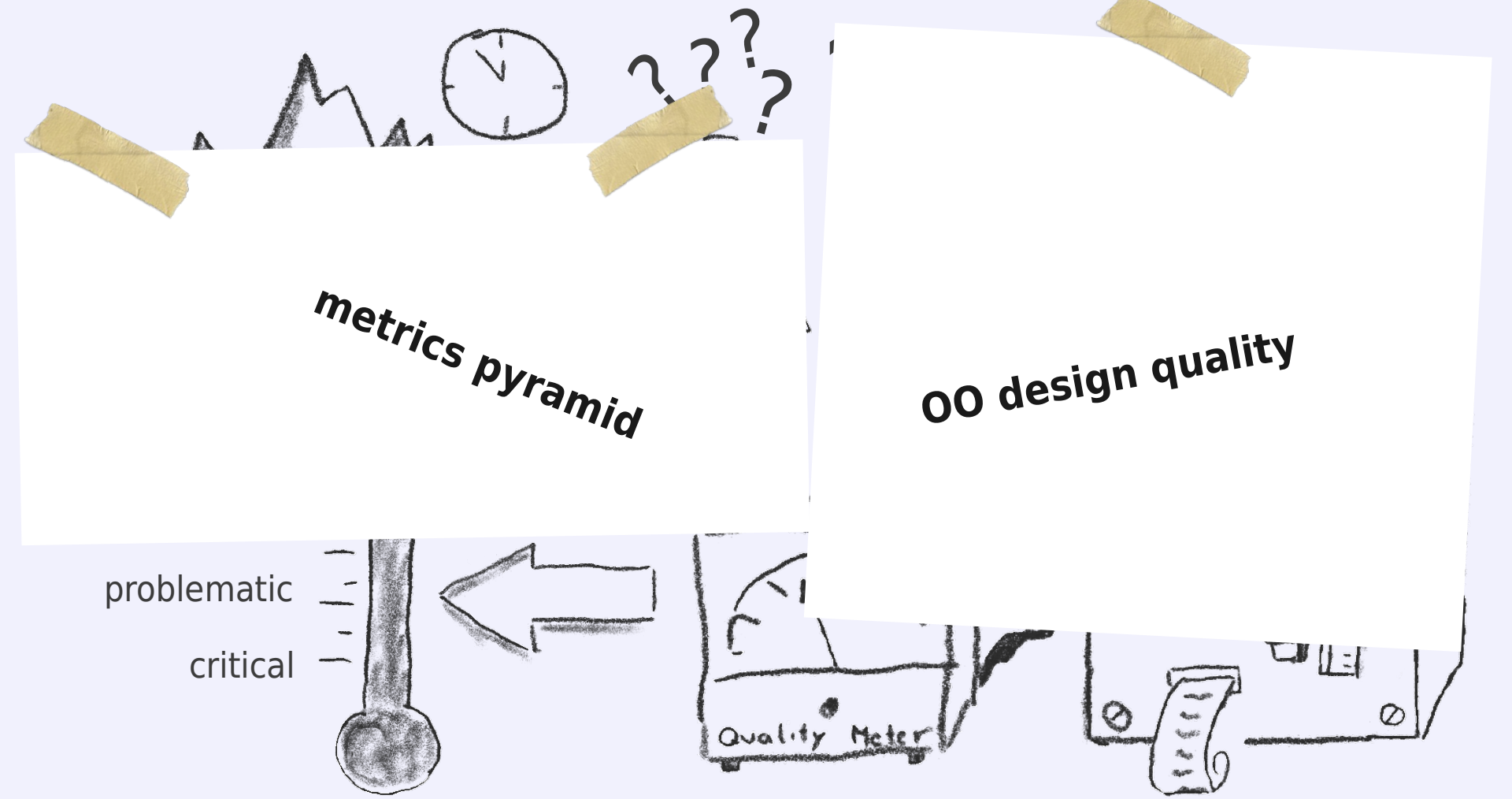
Complexity

using metrics...

OWASP
The Open Web Application Security Project

metrics pyramid

OO design quality



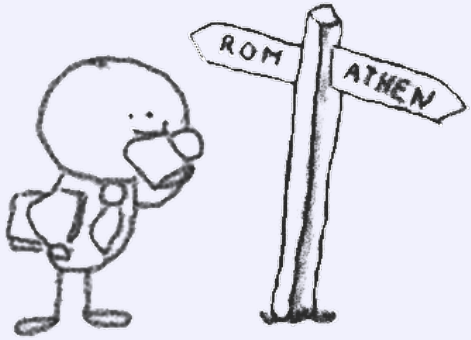
OWASP
The Open Web Application Security Project

lessons learned

Due Diligence Report

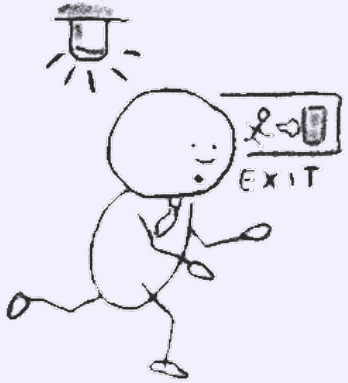
OWASP
The Open Web Application Security Project

Report often will not be read



Concrete recommendations are a must

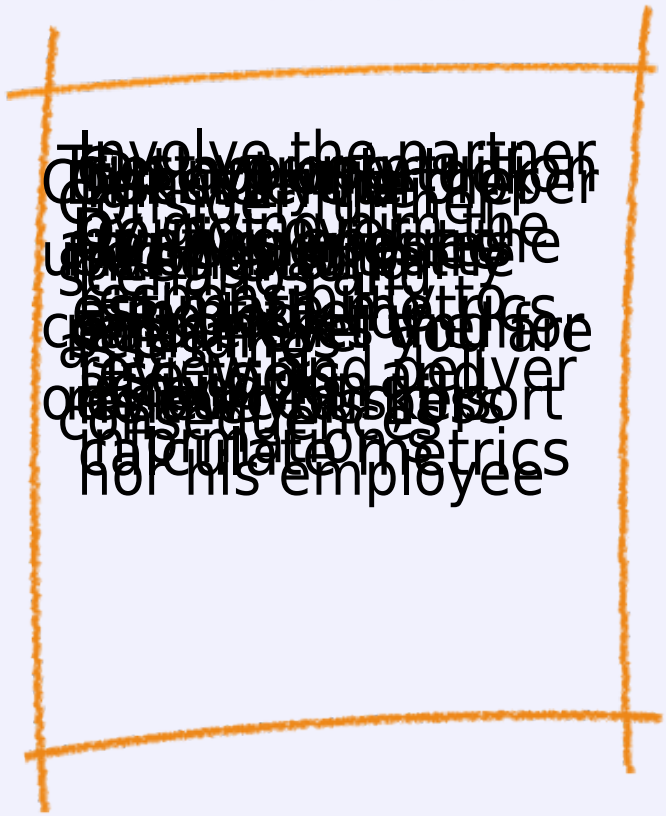
Visualisation helps a lot



Report will be read and used in political ways a lot, when problems show up

lessons learned...

OWASP
The Open Web Application Security Project



„Past success is your worst enemy”

OWASP

The Open Web Application Security Project

"Do not hire a man who does your work for money, but him who does it for love of it."

~ Henry David Thoreau