About Me

Dr. Amir Alsbih
Chief Information Security Officer
CISSP-ISSMP
GCFA
E-Mail: amir.alsbih@haufe-lexware.com
Twitter: @checkm4te
Technical Due Diligence?
"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
• 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
...but what about the Hard- and Software-Systems?
but think about

Analysis and assessment of the software and hardware landscape should be considered from the beginning of the due diligence process.

In regard to other aspects, the assessment of these aspects is more complicated.

Software is not viewable, not tangible, and cannot be measured directly. Software changes permanently and always has errors.

Hardware will fail, and no software can exist without hardware.

Complex Eco Systems are connected to the world.
so what is the story?
Please tell the weight of this building based on the image

... To difficult?

Then please tell the height of the building (tolerance <1%)
so what is our job?
The goals are...

- Complexity
- Processes
- Scalability & Reliability
- Maintainability
- Information Security
- Know-How & Skills
- Third-Party
- Integration & Openness
a view from 30,000 feet...
how do we get there?
Quality attributes:

**Usage**
- Usability
- Localization
- Accessibility
- Personalization
- Customizability

**Development**
- Manageability
- Maintainability
- Supportability
- Extensibility
- Flexibility

**Operations**
- Performance
- Reliability
- Availability
- Scalability

**Security**
- Attacks
- Privacy
- Misuse
- Legislation
how to measure?

OWASP
The Open Web Application Security Project

functionality
reliability
usability
performance
attacks
costs
scalability
architecture
coupling
extensibility
security
coding practice
testability
reusability
openness
flexibility
maintainability
complexity
legislation
our current approach...
Software Architecture
“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

Reliability

Performance

Security

Functionality

Usability
there are no ugly babies!
have you seen this before?

Golden Hammer
Lava Flow
Wheel Factory
Stove Pipes
Internal Platform
Gas Factory
no easy going...
real world constraints...

- Confidentiality
- Documentation
- Expert Knowledge
- Time Frame
- Complexity
using metrics...

metrics pyramid

problematic
critical

OO design quality
lessons learned
Due Diligence Report

Report often will not be read.

Visualisation helps a lot.

Concrete recommendations are a must.

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

Get a proper briefing about the aim of the acquisition. Talk with the partner on an equal level; you are neither his boss nor his employee. Don't only look for weaknesses; also look for strengths. Consider further integration scenarios and assess the consequences. Consider further integration scenarios. Discuss your findings with the partner; let them review your report. Involve the partner by giving him the responsibility to review and deliver information. Use tools and calculate metrics. Do not overestimate metrics. Check for the proper use of third-party components and for outsourced skills. Trust your intuition and experience.

„Past success is your worst enemy”
“Do not hire a man who does your work for money, but him who does it for love of it.”

~ Henry David Thoreau