



Security as a Part of Quality Assurance.

The world would be a better place, if...

2008-11-19

Table of contents.

- Person who defines requirements, knows what they should 3
 - Decision & Cost estimation 4
- Persons who makes development planning, knows what they should 5
 - Planning & Methods 6
- Persons who are developers of software, do what they are able and do it right 7
 - Development & Model 8
- Persons who tests systems, knows what they need to do 9
 - Testing 10
- Persons who use systems, does only what they should do 11
 - Usage 12
- And when something unwanted happens, we all know how we should react. 13
 - Maintenance & Monitoring 14
- Thank you. 15

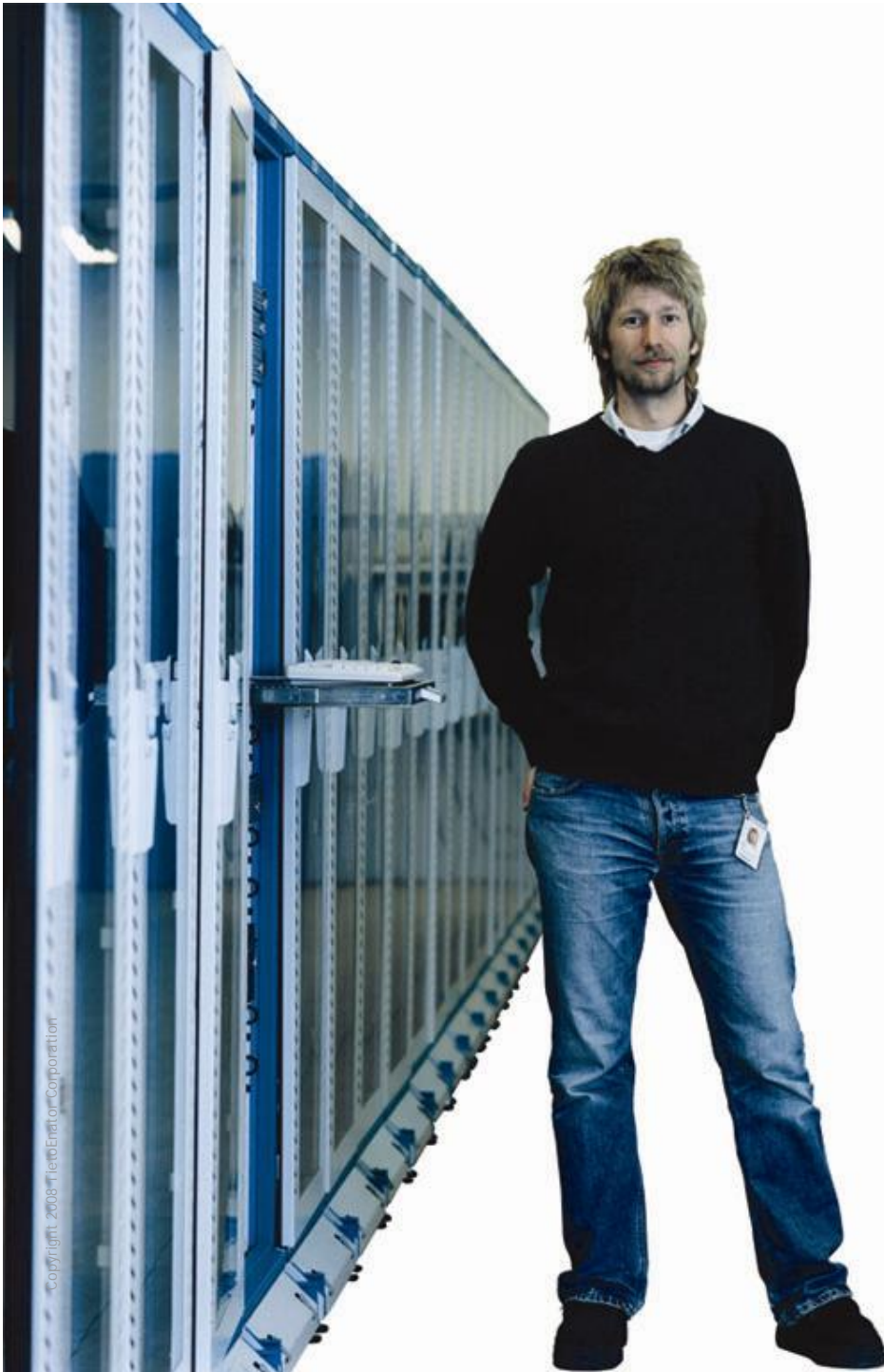


Person who defines requirements,
knows what they should
Decision & Cost estimation

Decision & Cost estimation

- What will be purpose of new system or service?
 - What kind of user profiles there are? Who are they?
 - What are the business functions that are served by new service?
 - How business function and tasks works?
 - What will be benefit of new service? ROI?
 - Are there regulations or law elements that need to be considered?
- Purpose:
 - Local
 - Internal
 - Extranet
 - www
 - Users
 - Inside
 - Partners
 - Customer
 - Any
 - Effectiveness
 - Work
 - Financial
 - PR

Decision is not allowed to be made only because it CAN be done.



Persons who makes development
planning, knows what they should
Design & Architecture

Design & Architecture

- What are the systems that needs integration?
 - What is information that need to be exchanged? With who?
 - What will be most suitable infrastructure for service?
 - What technical solutions we have in use?
 - What components we already have in use?
 - Is time schedule and resource allocation reasonable? Tools?
- Design
 - Data
 - Frequency
 - Encryption
 - Signature
 - Validation
 - Technical plan
 - Use centralized services
 - Think components and service, not code and procedures.
 - Framework that is in use (Tools)
 - Resources
 - Technical knowledge base
 - Time
 - Persons (knowledge)
 - Software assets

No need to plan - we have done this before.



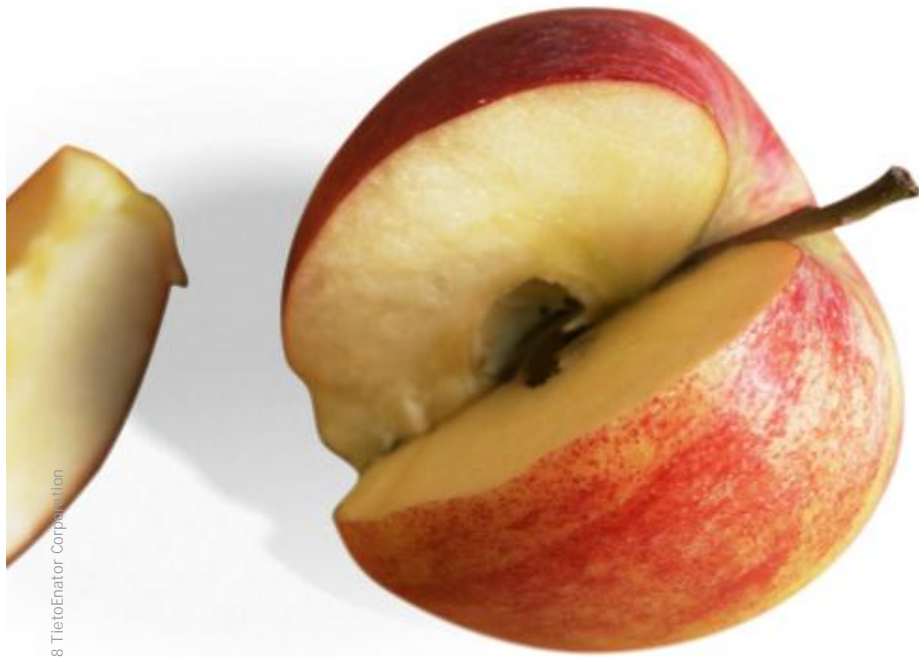
Persons who are developers of software, do what they are able and do it right

Development & Model

Development & Model

- What tools are used in development?
- How tools are used? Is there Framework?
- How is version management done?
- How is documentation stored?
- How are reviews done?
- Is there cross check method in use?
- What is the development method?
- Only approved tools are allowed to use.
- Split service to components.
- Components must do what they should and nothing else.
- Pay attention to
 - Authentication
 - Accessing data
 - Modification of data
- Cross check after self test
- Do not forget user.

I made proto - We take it to production.



Copyright 2008 TietoEnator Corporation

Persons who tests systems, knows what
they need to do
Testing & Evaluation

Testing & Evaluation

- Is there testing support tool in use?
- Is there test plan?
- Is test data real?
- What test is expected to approve?
- What are controls in testing environment?
Are they effective?
- Is test environment insulated?
- Use right test for purpose
 - Accuracy (Result & Parameters)
 - Performance (Capacity)
 - Usability (Supporting business)
 - Availability (Smoke test)
- What to test:
 - Input (parameters)
 - Authentication process
 - Functionality (Correct result)
 - Service call's and information exchange
 - Audit functions
 - Backup and Restore
- Purpose of test is to support decision making
- Never create connections between test and production services.
- Use dedicated user accounts in tests.

I did it, I test it, now it is working correctly.



Persons who use systems, does only
what they should do
Users

Users

- Can users do what they need to do?
- Do users has required knowledge to perform actions?
- How users really uses system to get work done?
- Is support supporting users as they need?
- Is user life cycle well managed?
- Do you know who is using your system?
- Define and maintain user profiles
 - Main user
 - User group A to Z
 - External users
 - Anonymous users
- Use Identity Management
 - Manual or Automatic
 - Source ID data
 - Access groups and recourses
 - Workflow (request-accept-grand->revoke)
 - Tracking
- Agility to tune
- Guide and information
- Reviews and questioners

We got new organization, people do what they used to do.

And when something unwanted happens, we all know how we should react.

Maintenance & Monitoring



Maintenance & Monitoring

- Can you identify error in system?
- Can you identify misuse of system or recourses?
- Can you be sure that system is available?
- Can system be recovered as planned?
- Who to inform and how?
- Does control cover whole running time?
- Monitoring requires
 - Manual or Automatic
 - Definition (Why)
 - Countermeasures (What)
 - Action plan (How)
- Incident management process
- Problem management process
- Patch management process
- Change management process
- ITIL will help, but not resolve anything

Red light, Red light - Lets go to lunch

Thank you.

... then there won't be any security issues.