INTEGRATING SECURITY TESTING, RISK ASSESSMENT AND COMPLIANCE ASSESSMENT

© Matthias Heyde / Fraunhofer FOKUS

TAROT Summer School, Paris 2016

Jürgen Großmann, Fraunhofer FOKUS

Engineering a Connected World

The results presented here have been developed as part of the projects RASEN and PREVENT. The project RASEN is granted by the EU in the Seventh Framework Program. The project PREVENT is funded by d the Federal Ministries of Education and Research (BMBF) in Germany.

FRAUNHOFER FOKUS

- 434 employees
- Established in 1987
- 56 EU projects
- Approx. 100 industry partners
- Approx. 200 industry projects
- 6 patents granted

© Michael Zalewski / Fraunhofer FOKUS

Fraunhofer FOKUS

FOKUS STANDS FOR …

… significant contributions to information and communication technologies:

- IP telephony: SIP
- Future internet and autonomic communication: IMS, EPC, M2M
- Future media: HTML5, IPTV, DASH, Smart TV
- eGovernment: Digital Public Services
- Automotive: Autosar, Car2X, connected driving
- Model-driven engineering: UML, MOF
- Test automation and system quality: TTCN-3, MBT, UTP
- Networked security: KATWARN
- Visualization: automatic calibration of projection systems

©Matthias Heyde / Fraunhofer FOKUS

QUALITY ENGINEERING – SQC

SQC ensures quality and reliability across domains in the transformation process towards digital networked systems.

Topics:

– Cost efficient quality for networked systems
– System and software architectures
– Cyber security and safety
– Risk analysis and risk management
– Model based system development
– Testing and verification
– Process analysis and process optimization
– Automation and tool integration
– Support in certification

© Matthias Heyde/ Fraunhofer FOKUS

AGENDA

1. Motivation

2. Introduction to **security risk assessment**

3. Introduction to **risk-based security testing**

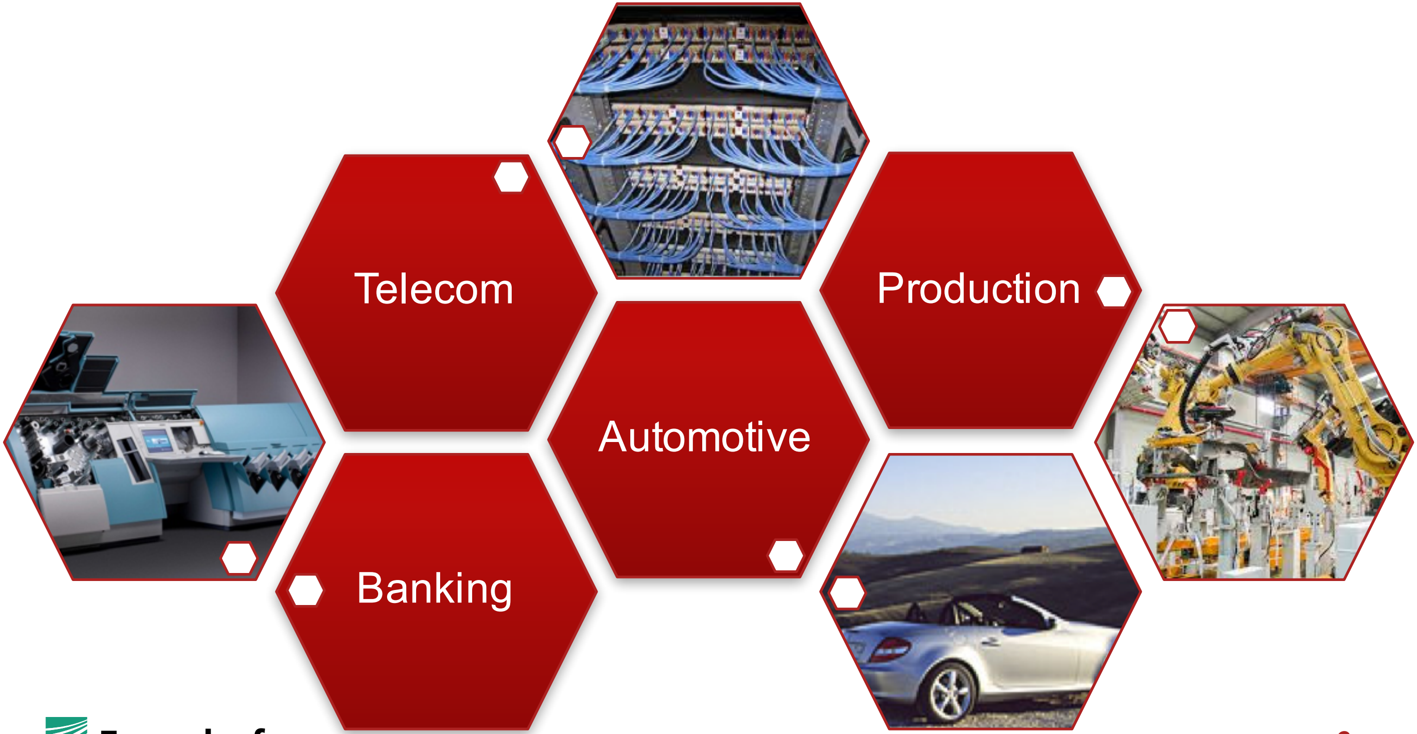
4. The RASEN approach: **combining compliance assessment, security risk assessment and security testing**

5. Tool support and **standardization**

6. Outlook

SOFTWARE IS OMNIPRESENT

… and affects your personal and business life



Telecom

Production

Automotive

Banking

Fraunhofer
FOKUS

IT SECURITY IS A MUST FOR MODERN ICT INFRASTRUCTURES

ICT infrastructures need to maintain a high level of information security

- Business criticality
- Critical infrastructures (critical for society)
- Critical for human well-being and life (safety)
- Deal with private and other sensible data
- Growing number of laws, legally motivated rules and other regulations

© Holger Mette / iStockphoto

Fraunhofer FOKUS

Risk

System quality

Compliance

Technical decisions may imply legal and security risk and compliance issues and security issues may affect technical decisions.

Source: https://www.flickr.com/photos/maerskline/8432240103/in/photostream/
License: https://creativecommons.org/licenses/by-sa/2.0/

IT SECURITY RISK

Definition

The Potential that a **threat** will exploit a **vulnerability** of an **asset or group of assets** and thereby cause harm to the organization *(Source ISO 27000)*

Risk = Likelihood * Consequence

Fraunhofer
FOKUS

PEOPLES‘ RISK PERCEPTION IS USUALLY BAD

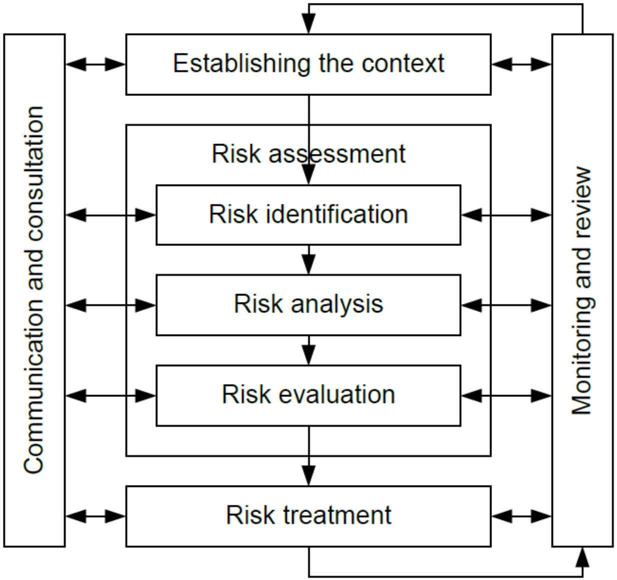
- Over-estimate intentional threats and underestimate accidents
- Over-react on things that offend our moral
- Over-estimate immediate threats in comparison long-term or slow threats
- Blind-spotted by own habits and perspectives

(Schneier on Security)

RISK ASSESSMENT PROCESS

ISO 31000 / 2009

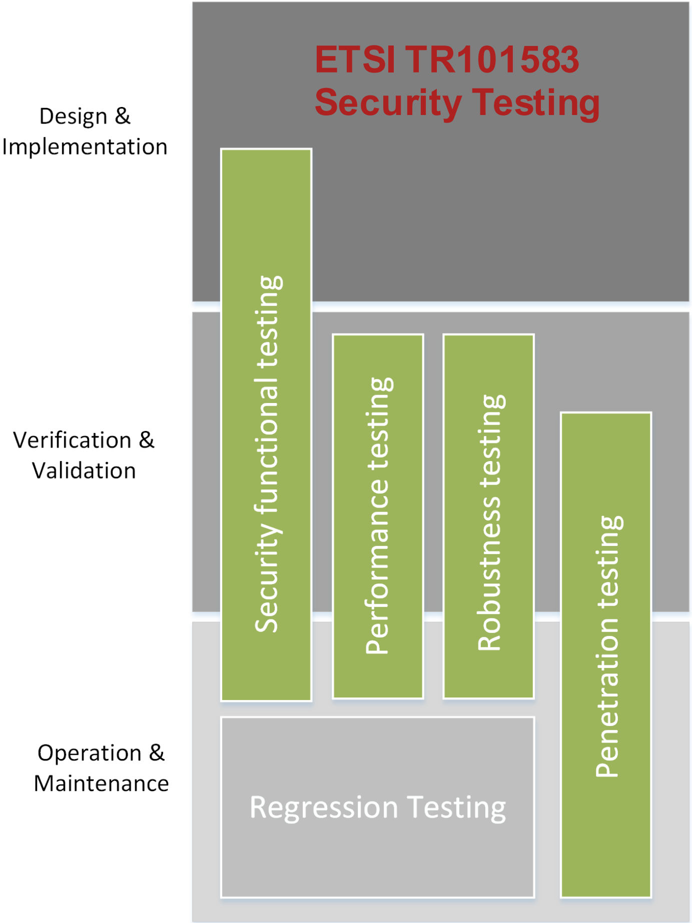
- **Risk identification:** identifying sources of risk, areas of impacts, events, their causes and their potential consequences
- **Risk analysis:** comprehend the nature of risk and to determine the level of risk
- **Risk evaluation:** comparing the results of risk estimation with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
- **Risk treatment:** modify risk by avoidance or mitigations



SECURITY TESTING

ISO 29119 Dynamic Test Process

- **Test planning:** determine test strategy, resource planning
- **Test design :** deriving the test cases and test procedures.
- **Test implementation:** realizing the executable test scripts.
- **Test execution:** running the test procedure resulting from the test design and implementation phases.
- **Test reporting:** managing the test incidents and the test results.



Fraunhofer FOKUS

COMPLIANCE ASSESSMENT

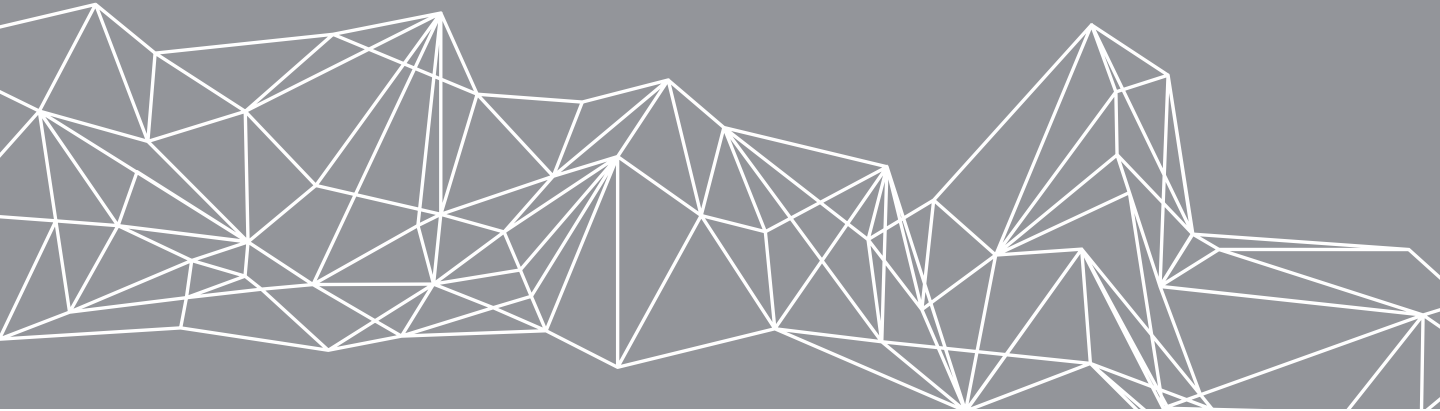
Compliance to laws and legal norms become more and more relevant

- Security and privacy have become significant areas of concern for legislators over the past few years
  - EU Network Information Services (NIS) Directive
  - EU data protection rules (**General Data Protection Regulation (GDPR)** 2016/679)
  - National initiatives like German IT Security Act
- Regulatory fines for breach of security are becoming increasingly stringent.

1. Identify compliance requirements
2. Identify compliance issues
3. Evaluate compliance issues

By Gambrus (own work, using Image:Emblem-important-red.svg) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

SECURITY RISK ASSESSMENT



... an intuitive approach

Engineering a Connected World

Fraunhofer
FOKUS

THE HBGARY HACK 2011

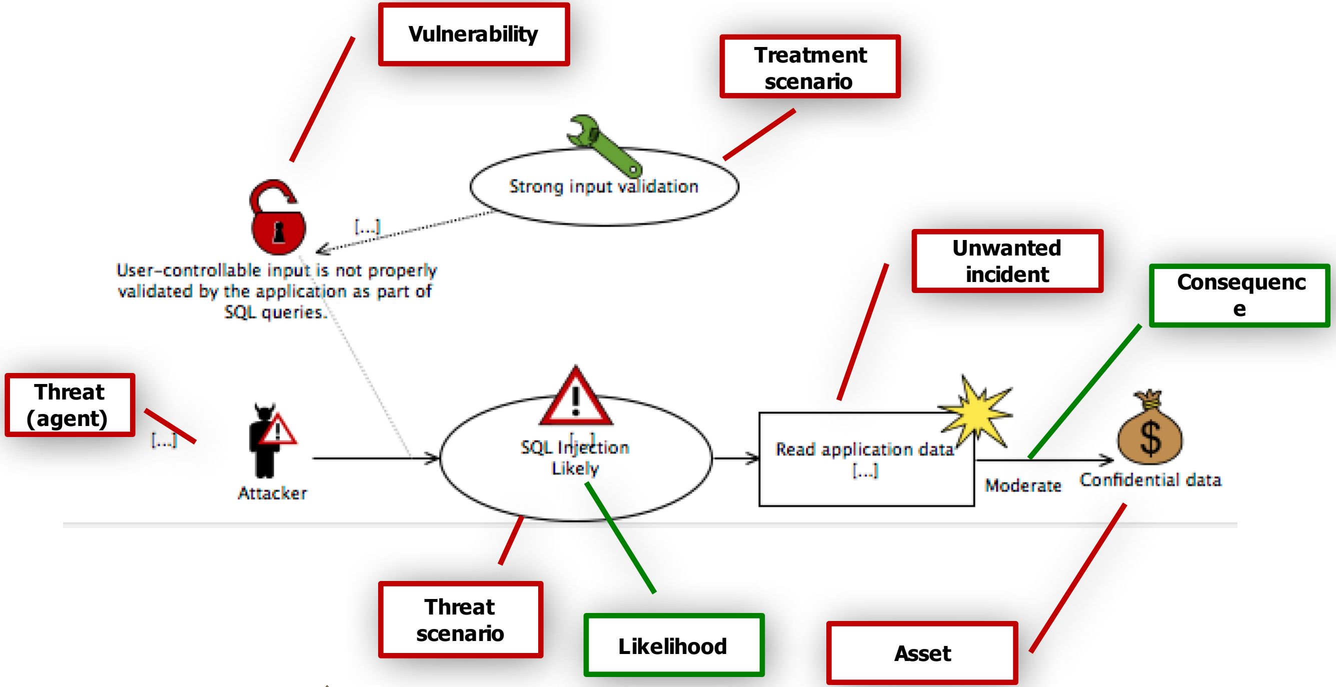
A clever combination of dependent exploits

	Attack Method	Attacked System	Vulnerability	Lost Assets
1	SQL Injection	CMS on HBGary Federal's website, hbgaryfederal.com	CMS with missing validity check of SQL parameters	List of usernames, e-mail addresses, and password hashes of the HBGary employees
2	Password cracking using rainbow tables	Password hashes from 1	Hashes without salt, weak passwords	clear text passwords
3	Unauthorized use of passwords from 2	E-mail, Twitter accounts, and LinkedIn accounts of HBGarry officials	Password double use	Email accounts of HBGary officials
4	Unauthorized use of passwords from 2	Machine running support.hbgary.com	Password double use	Non-superuser account of HBGary official
5	Privilege escalation	Machine running support.hbgary.com	Privilege escalation vulnerability, system not up to date	Full access to HBGary's system, gigabytes of backups and research data
6	Social engineering	Machine running rootkit.com	Credulous staff	Integrity of rootkit.com

Source: http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/

MODEL-BASED SECURITY RISK ASSESSMENT

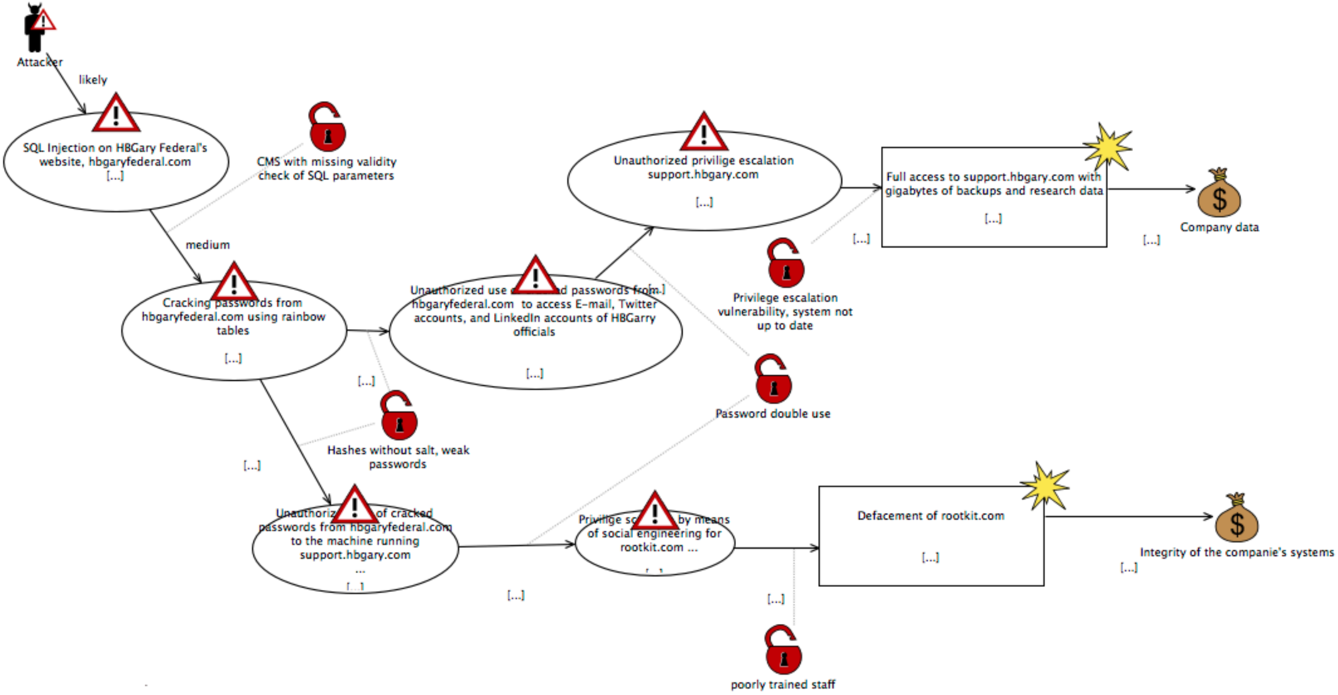
The CORAS approach



Bildquelle http://coras.sourceforge.net/

THE HBGARY HACK

… modeled with CORAS



Attacker

likely

SQL Injection on HBGary Federal's website, hbgaryfederal.com [...]

CMS with missing validity check of SQL parameters

medium

Cracking passwords from hbgaryfederal.com using rainbow tables [...]

Hashes without salt, weak passwords

[...]

Unauthorized use o d passwords from hbgaryfederal.com to access E-mail, Twitter accounts, and LinkedIn accounts of HBGarry officials [...]

[...]

Unauthorized privilige escalation support.hbgary.com [...]

Privilege escalation vulnerability, system not up to date

Password double use

Full access to support.hbgary.com with gigabytes of backups and research data [...]

[...]

Company data

[...]

[...]

Unauthoriz of cracked passwords from hbgaryfederal.com to the machine running support.hbgary.com ... [...]

[...]

Privilge sc by means of social engineering for rootkit.com ... [...]

[...]

poorly trained staff

Defacement of rootkit.com [...]

Integrity of the companie's systems

[...]

RISK EVALUATION

Risk = rv (Likelihood, Consequence)

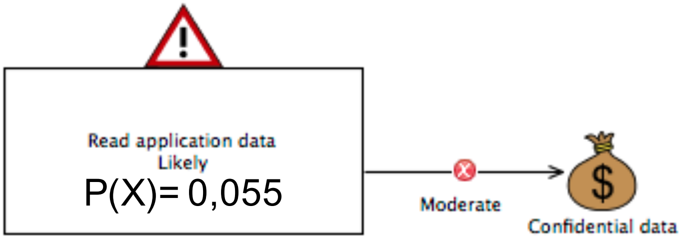
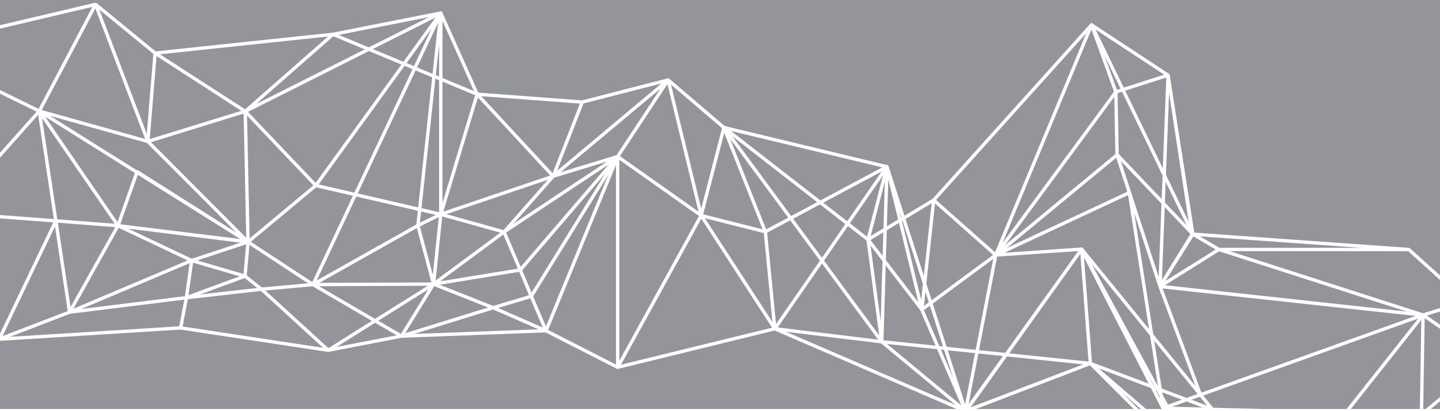


Table 1 Risk Function for Base Incidents

		Consequences			
		minor	***moderate***	***major***	***catastrophic***
Likelihood	< ***0.03***	very low	very low	low	medium
	[0.03-0.06[	very low	low	medium	high
	[0.06-0.16[	Low	medium	high	very high
	≥ ***0.16***	Medium	high	very high	very high

RISK BASED SECURITY TESTING



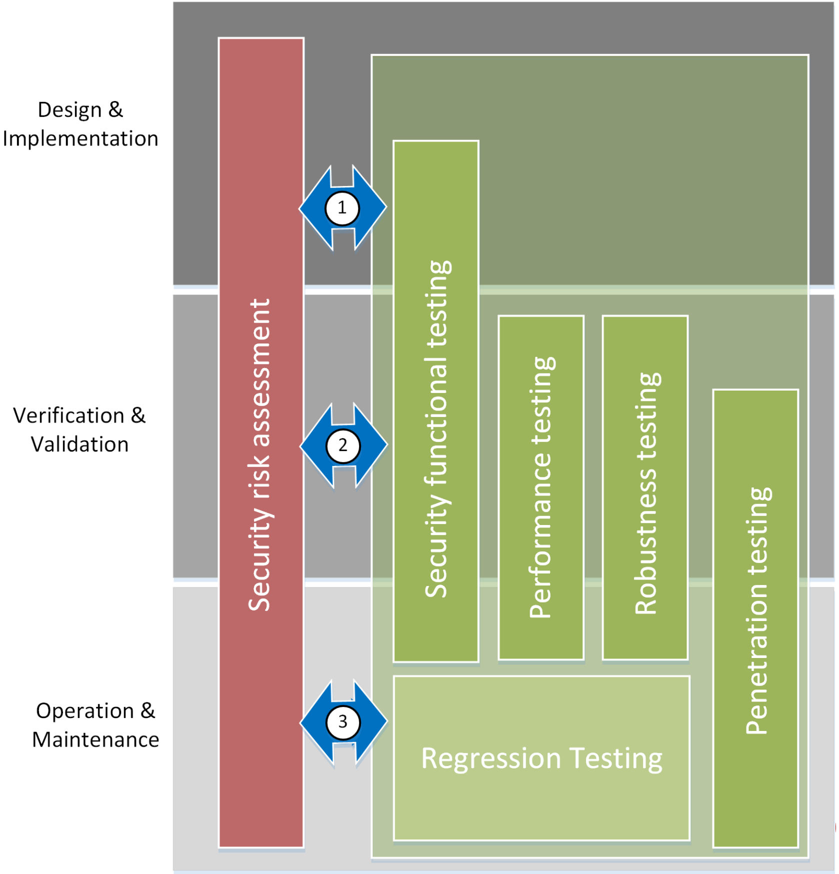
... an intuitive approach

Engineering a Connected World

Fraunhofer
FOKUS

RISK BASED SECURITY TESTING IN THE PRODUCT LIFE CYCLE

1. Rate security functional requirements and optimize the verification of their implementation by testing
2. Optimize test design and test implementation efforts, support for choosing the appropriate testing techniques
3. Optimize penetration testing and regression testing



Fraunhofer FOKUS

DIAMONDS

RISK-BASED SECURITY TESTING

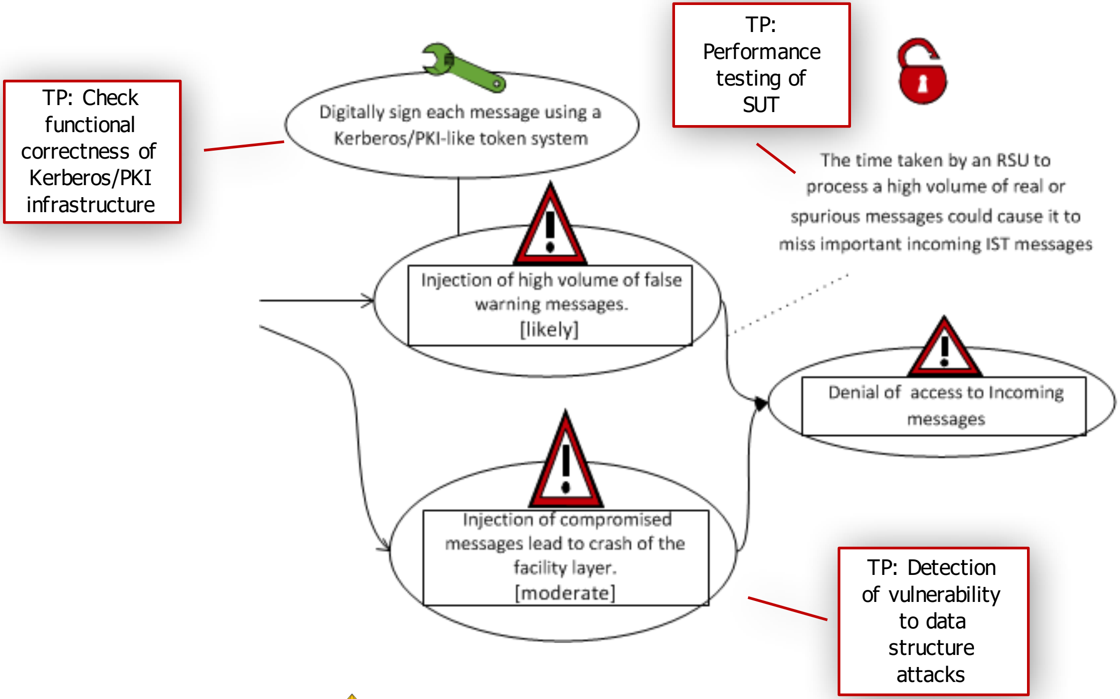
Qualitative and quantitative approaches

- **Qualitative approach:**
  - What and how should be tested?
  - Risk-based test identification
  - Risk-based test specification
- ***Artifacts:***
  - Vulnerabilities description
  - Threat scenarios
  - Treatment scenarios

- **Quantitative approach**:
  - How much/intensive should be tested?
  - How do I prioritize my testing resources?
  - Risk-based resource allocation
  - Risk-based test selection & prioritization
- ***Artifacts:***
  - Likelihood and consequence values

RISK-BASED SECURITY TEST IDENTIFICATION

Assigning test purposes to risk model elements


Digitally sign each message using a Kerberos/PKI-like token system
Injection of high volume of false warning messages. [likely]
Injection of compromised messages lead to crash of the facility layer. [moderate]
Denial of access to Incoming messages
The time taken by an RSU to process a high volume of real or spurious messages could cause it to miss important incoming IST messages

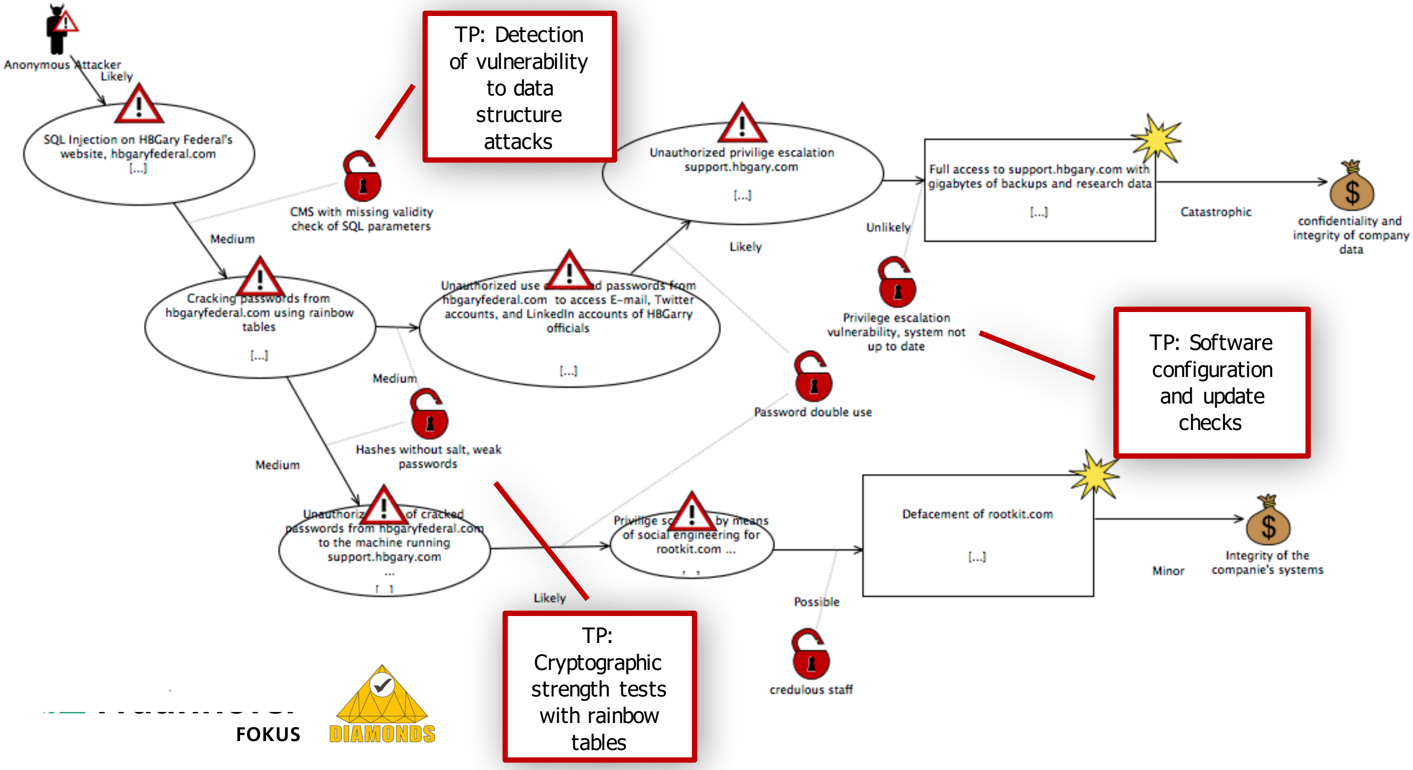
TP: Check functional correctness of Kerberos/PKI infrastructure

TP: Performance testing of SUT

TP: Detection of vulnerability to data structure attacks

RISK-BASED SECURITY TEST IDENTIFICATION

Assigning test purposes to risk model artifacts



TP: Detection of vulnerability to data structure attacks

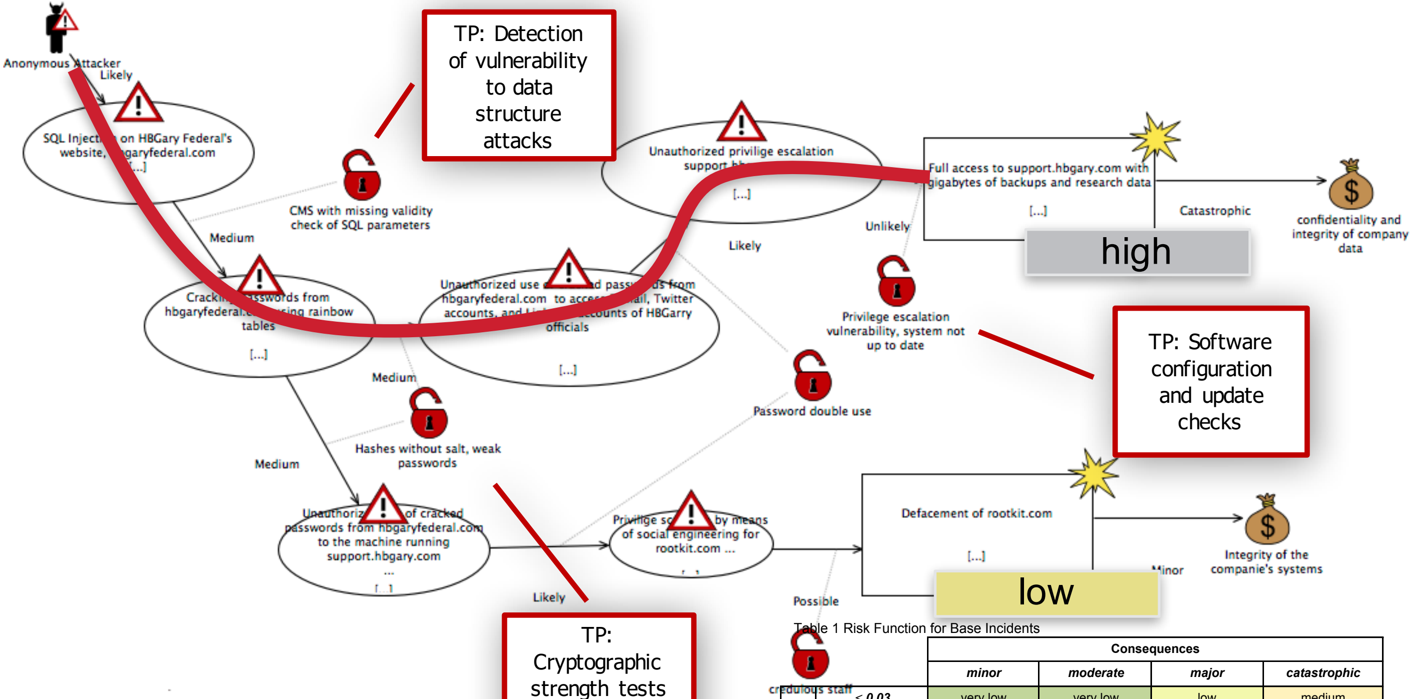
TP: Software configuration and update checks

TP: Cryptographic strength tests with rainbow tables

Anonymous Attacker
Likely
SQL Injection on HBGary Federal's website, hbgaryfederal.com [...]
CMS with missing validity check of SQL parameters
Medium
Cracking passwords from hbgaryfederal.com using rainbow tables [...]
Unauthorized use o d passwords from hbgaryfederal.com to access E-mail, Twitter accounts, and LinkedIn accounts of HBGarry officials [...]
Medium
Hashes without salt, weak passwords
Medium
Unauthoriz of cracked passwords from hbgaryfederal.com to the machine running support.hbgary.com ... [...]
Likely
Unauthorized privilige escalation support.hbgary.com [...]
Likely
Unlikely
Privilege escalation vulnerability, system not up to date
Password double use
Full access to support.hbgary.com with gigabytes of backups and research data [...]
Catastrophic
confidentiality and integrity of company data
Priviige sc by means of social engineering for rootkit.com ...
Possible
credulous staff
Defacement of rootkit.com [...]
Minor
Integrity of the companie's systems
FOKUS
DIAMONDS

SECURITY TEST PRIORITIZATION

Calculating overall risk contribution of items


Anonymous Attacker
Likely
SQL Injecti on HBGary Federal's website, garyfederal.com
[...]
CMS with missing validity check of SQL parameters
Medium
Crackin sswords from hbgaryfederal.c sing rainbow tables
[...]
Unauthorized use o d passw ds from hbgaryfederal.com to acce ail, Twitter accounts, and Li ccounts of HBGarry officials
[...]
Medium
Hashes without salt, weak passwords
Medium
Unauthoriz of cracked passwords from hbgaryfederal.com to the machine running support.hbgary.com
...
[...]
Likely
Privilge sc by means of social engineering for rootkit.com ...
[...]
Password double use
Unauthorized privilige escalation support.hb
[...]
Likely
Unlikely
Privilege escalation vulnerability, system not up to date
Full access to support.hbgary.com with gigabytes of backups and research data
[...]
Catastrophic
confidentiality and integrity of company data
high
Defacement of rootkit.com
[...]
Minor
Integrity of the companie's systems
low
Possible
credulous staff

TP: Detection of vulnerability to data structure attacks

TP: Software configuration and update checks

TP: Cryptographic strength tests with rainbow tables

Table 1 Risk Function for Base Incidents

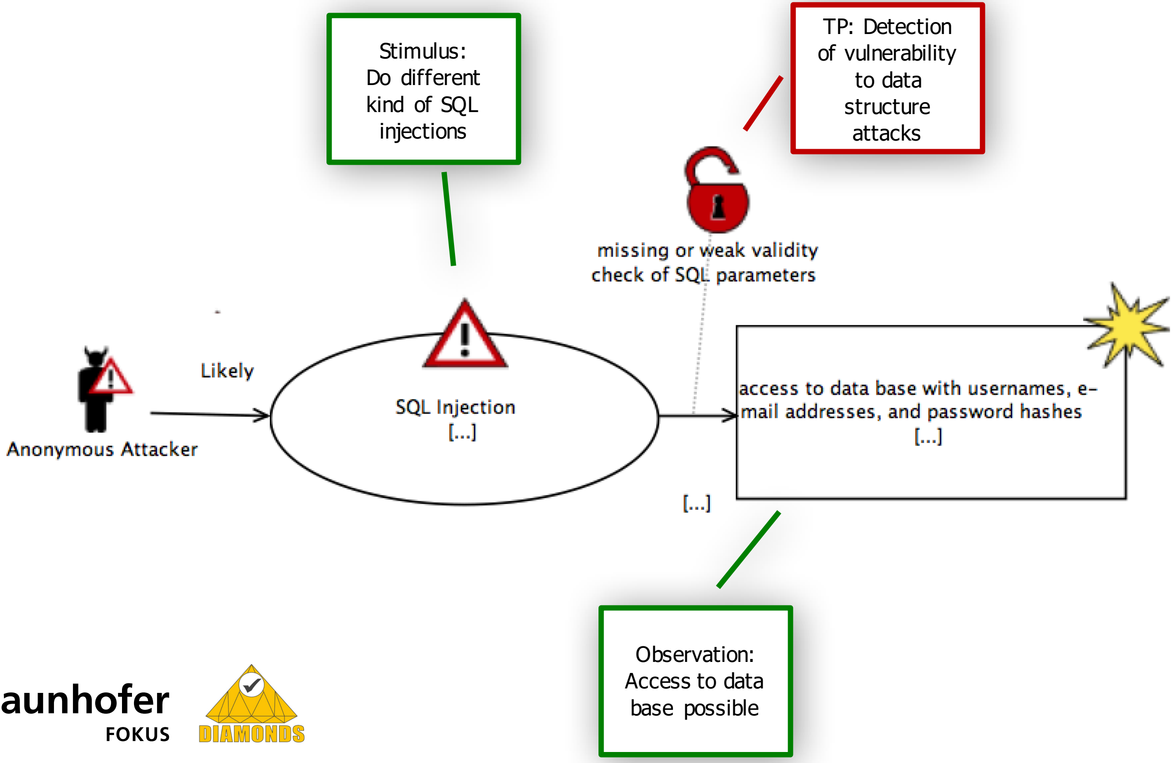
		Consequences			
		minor	moderate	major	catastrophic
Likelihood	< 0.03	very low	very low	low	medium
	[0.03-0.06[	very low	low	medium	high
	[0.06-0.16[	Low	medium	high	very high
	≥ 0.16	Medium	high	very high	very high

Fraunhofer FOKUS

DIAMONDS

RISK-BASED SECURITY TEST IDENTIFICATION

Decomposing the overall scenario


Likely
Anonymous Attacker
SQL Injection
[...]
missing or weak validity check of SQL parameters
access to data base with usernames, e-mail addresses, and password hashes
[...]
[...]

Stimulus: Do different kind of SQL injections

TP: Detection of vulnerability to data structure attacks

Observation: Access to data base possible

SECURITY TEST PRIORITIZATION

Calculating overall risk contribution of items

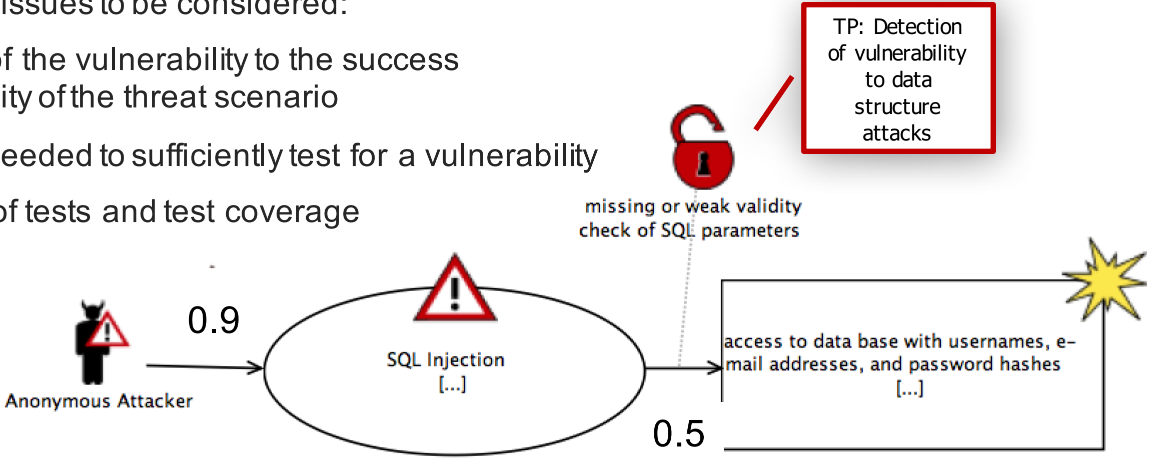
The potential that a **threat** will exploit a **vulnerability** of an **asset or group of assets** and thereby cause harm to the organization *(Source ISO 27000)*

Testing to find an **argument for the absence** of potential vulnerabilities.

- Calculate and rate the risks (probability of unwanted incidents * consequence).
- Identify the vulnerabilities with the highest impact to the most critical risks.

Additional issues to be considered:

- Impact of the vulnerability to the success probability of the threat scenario
- Efforts needed to sufficiently test for a vulnerability
- Quality of tests and test coverage



TP: Detection of vulnerability to data structure attacks

missing or weak validity check of SQL parameters

Anonymous Attacker

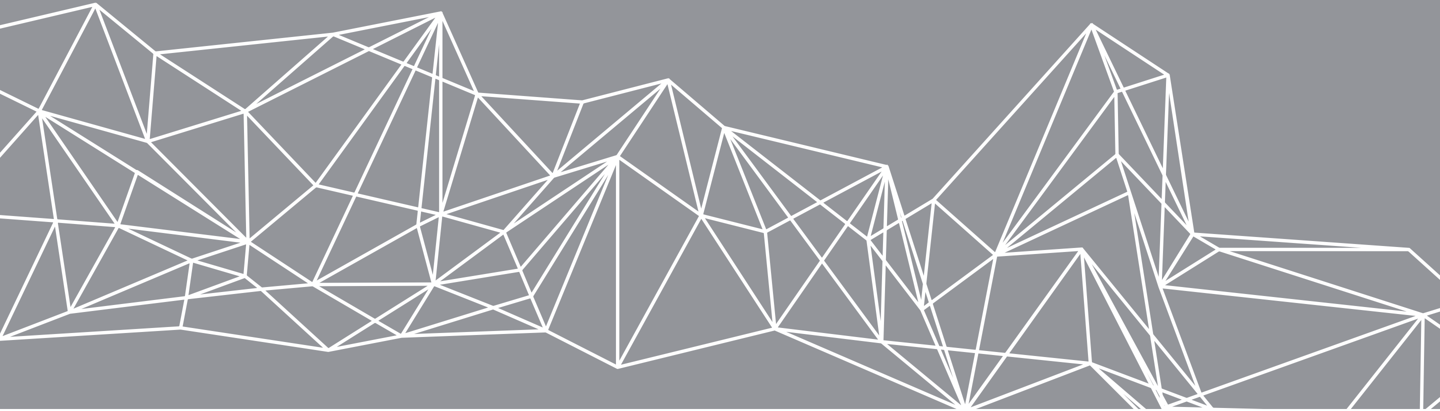
0.9

SQL Injection
[...]

0.5

access to data base with usernames, e-mail addresses, and password hashes
[...]

SYSTEMATICALLY COMBINE SECURITY TESTING, RISK ASSESSMENT AND COMPLIANCE ASSESSMENT



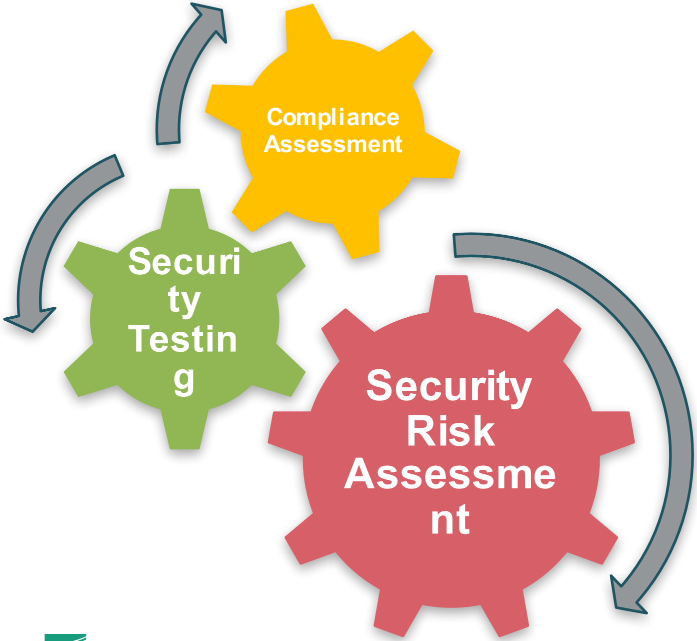
… addressing ISO 29119 and ISO 31000

Engineering a Connected World

Fraunhofer
FOKUS

FP7 PROJECT RASEN, BMBF PROJECT PREVENT

Developing methods and tools to support security assessments for large-scale networked infrastructures



Developing methods and tools to support **security assessments** for **large-scale networked infrastructures** by considering:

1. technical aspects
2. legal and regulatory aspects
3. uncertainty and risk

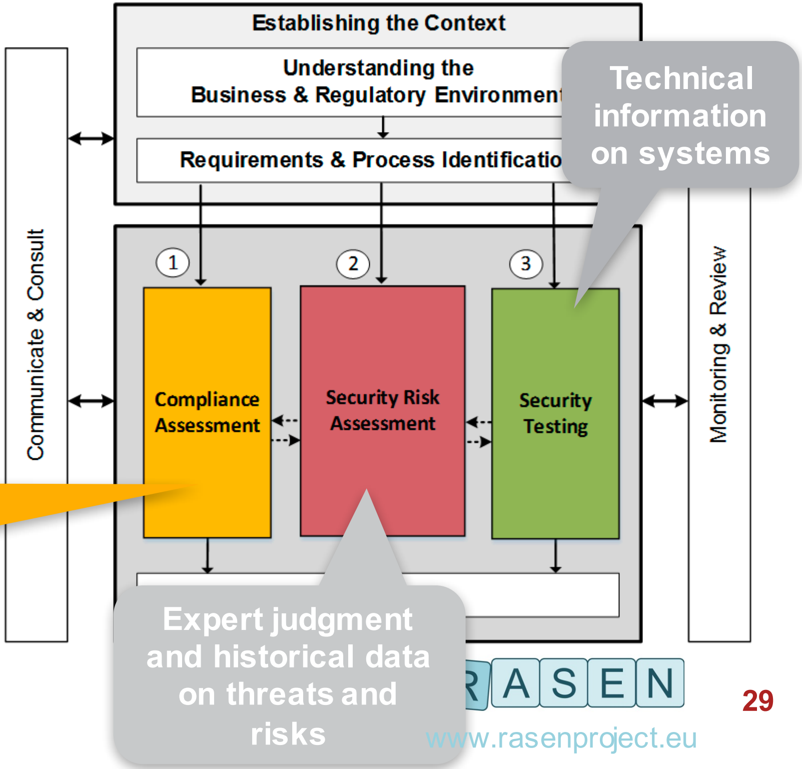
Fraunhofer FOKUS

RASEN
www.rasenproject.eu

A METHOD BASED ON STANDARDS

for security testing, risk & compliance assessment

- Conforms to ISO/IEC 31000 and ISO/IEC 29119
- Integrates risk assessment, compliance assessment and security testing in a meaningful manner
- Addresses management aspects as well as assessment aspects



Legal rules regarding systems and processes

Expert judgment and historical data on threats and risks

Technical information on systems

Fraunhofer FOKUS

www.rasenproject.eu

RASEN METHOD'S MAIN WORKSTREAMS

A risk-based compliance assessment workstream

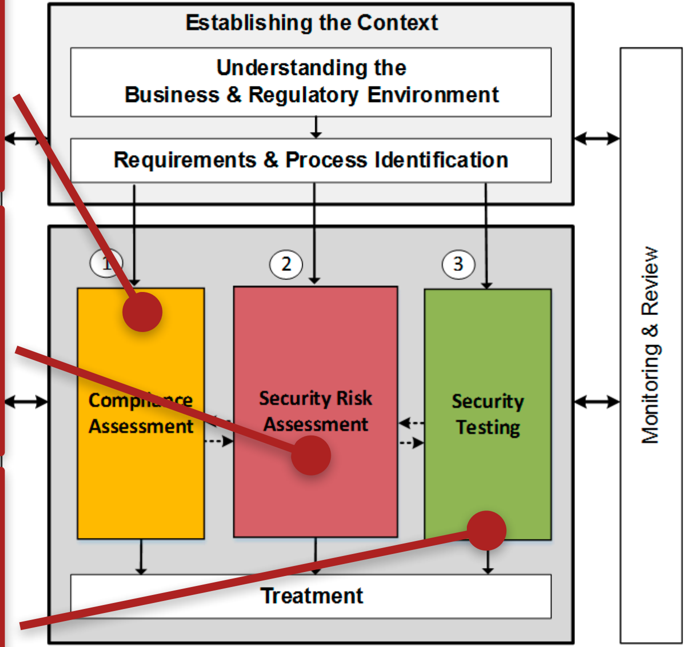
- focus the compliance resources on the areas that are most likely to cause concern
- building and prioritizing the compliance measures around the identified risks.

A test-based security risk assessment workstream

- starts with the risk assessment
- optimizes security risk assessment with empirical data coming from test results or compliance issues.

A risk-based security testing workstream

- facilitates test generation from attack pattern and test pattern
- focus security testing on the areas that are most likely to cause concern
- building and prioritizing the testing program around the identified risks.



www.rasenproject.eu

Test based security risk assessment

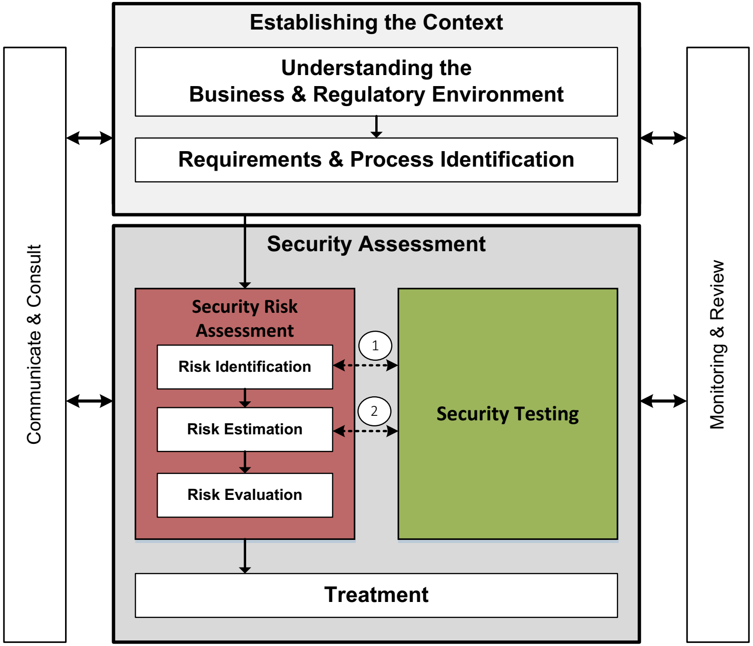
Engineering a Connected World

Fraunhofer
FOKUS

TEST-BASED SECURITY RISK ASSESSMENT

Basic idea: improve risk assessment activities through facts from testing

1. Test-based risk identification
2. Test-based risk estimation

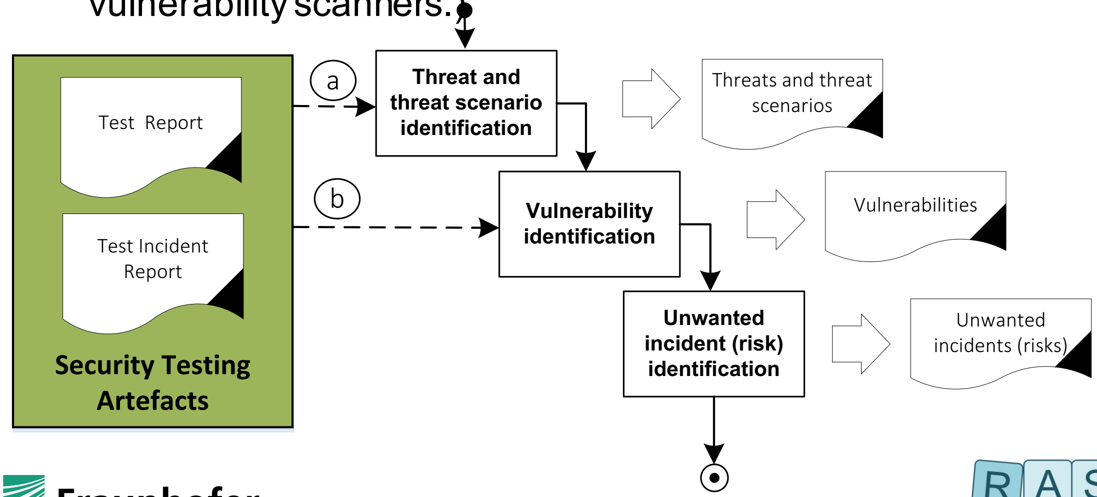


TEST-BASED RISK IDENTIFICATION

Using testing and and automated scanning to systematically discover the attack surface

a) **Test-based attack surface analysis** (interfaces/entry points by network discovery tools, web-crawlers, and fuzz testing tools)

b) **Test-based vulnerability identification** (penetrating testing tools, model-based security testing tools, static and dynamic code analysis tools, and vulnerability scanners.)



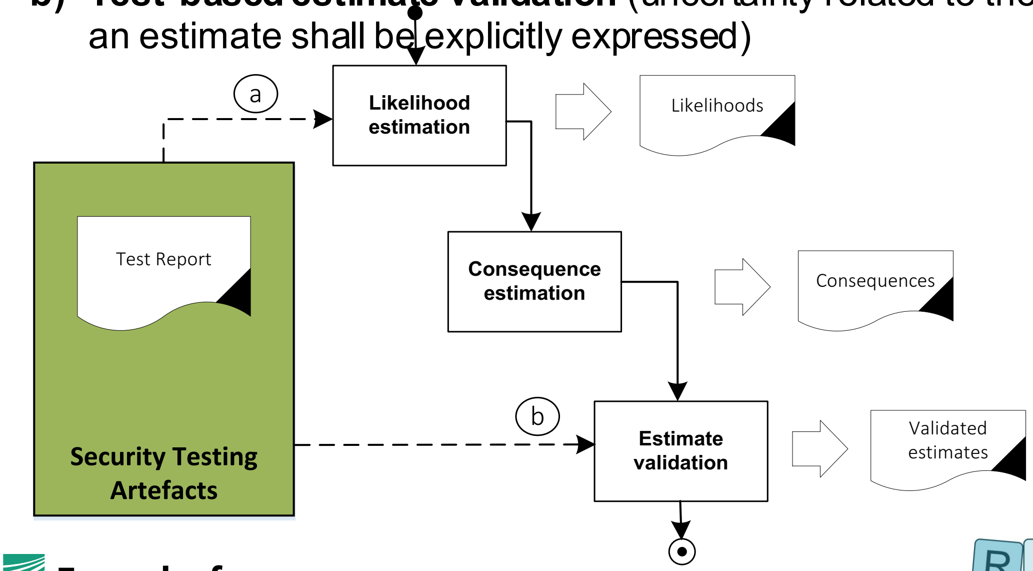
Test Report
Test Incident Report
Security Testing Artefacts
a
b
Threat and threat scenario identification
Threats and threat scenarios
Vulnerability identification
Vulnerabilities
Unwanted incident (risk) identification
Unwanted incidents (risks)

TEST-BASED RISK ESTIMATION

Using testing to systematically improve and validate the estimates

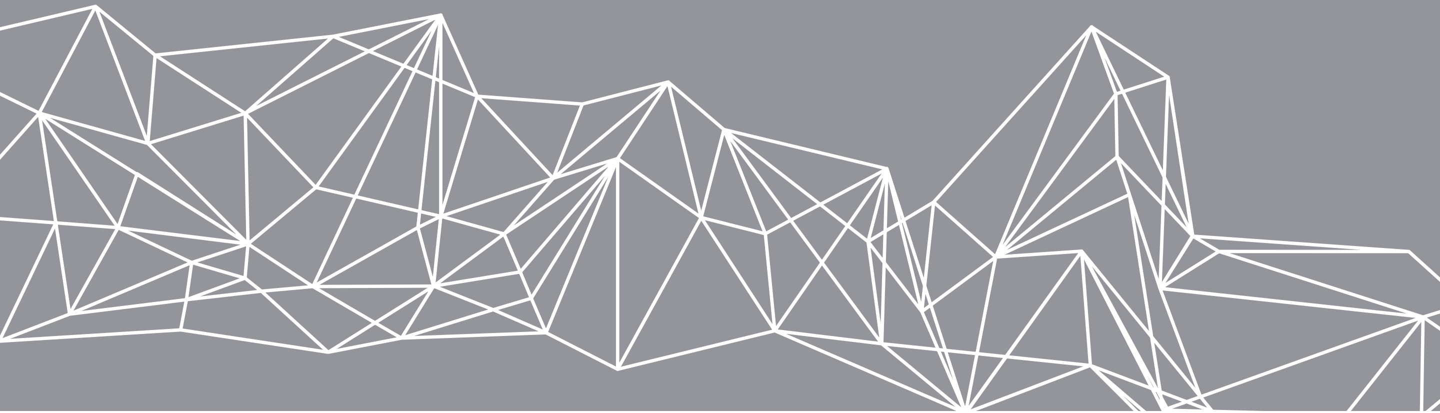
a) **Test-based likelihood estimation** (likelihood that an attack will be successful if initiated)

b) **Test-based estimate validation** (uncertainty related to the correctness of an estimate shall be explicitly expressed)



Fraunhofer FOKUS

RASEN www.rasenproject.eu



Risk based security testing

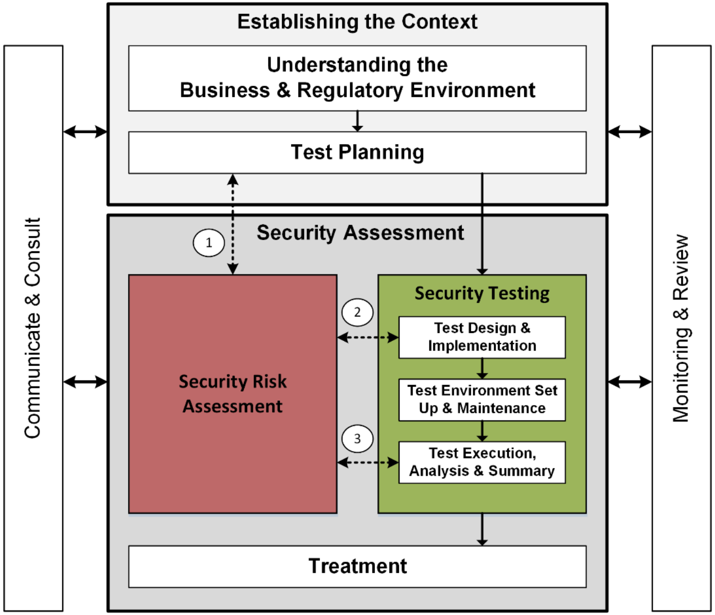
Engineering a Connected World

Fraunhofer
FOKUS

RISK-BASED SECURITY TESTING COMPLIANT TO ISO 29119

Basic idea: focus testing activities on high risk areas

1. Risk-based security test planning
2. Risk-based security test design & implementation
3. Risk-based test execution, analysis & summary


Establishing the Context
Understanding the Business & Regulatory Environment
Test Planning
Communicate & Consult
Monitoring & Review
Security Assessment
1
2
3
Security Risk Assessment
Security Testing
Test Design & Implementation
Test Environment Set Up & Maintenance
Test Execution, Analysis & Summary
Treatment

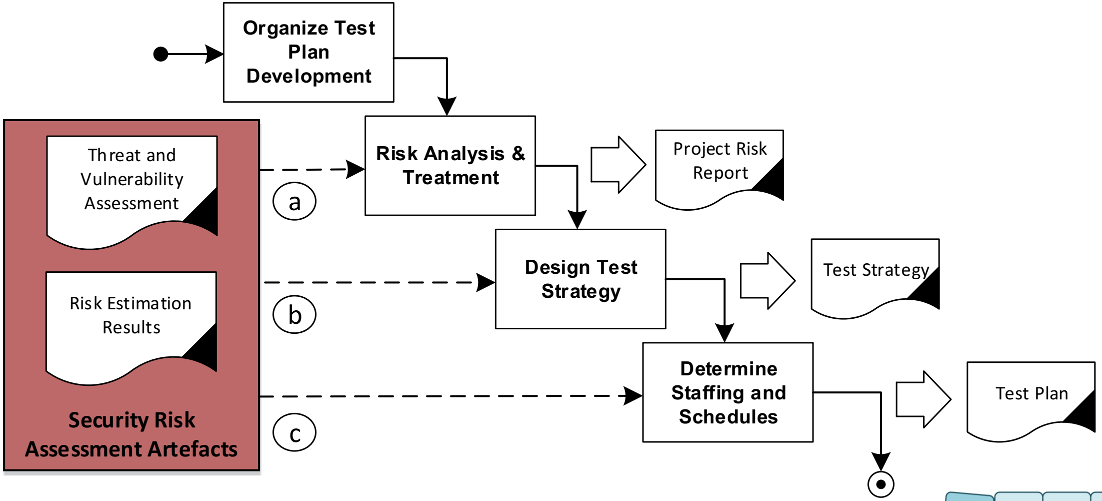
Fraunhofer FOKUS

RASEN
www.rasenproject.eu

RISK-BASED SECURITY TEST PLANNING

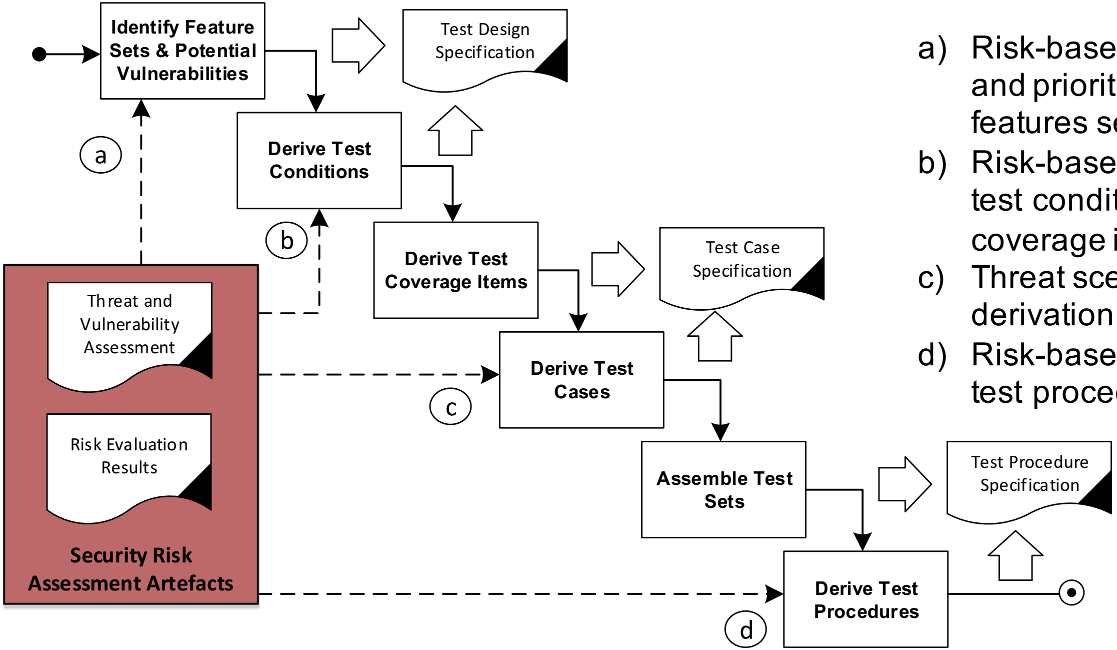
Determines the test objective, the test scope, and the risks associated to the overall testing process

a) Integrate risk analysis
b) Risk-based test strategy design
c) Risk-based security resource planning and test scheduling


Organize Test Plan Development
Threat and Vulnerability Assessment
Risk Estimation Results
Security Risk Assessment Artefacts
a
b
c
Risk Analysis & Treatment
Project Risk Report
Design Test Strategy
Test Strategy
Determine Staffing and Schedules
Test Plan

RISK-BASED SECURITY TEST DESIGN AND IMPLEMENTATION

Systematically prioritize and derive security test cases



Identify Feature Sets & Potential Vulnerabilities
Test Design Specification
Derive Test Conditions
a
b
Derive Test Coverage Items
Test Case Specification
Threat and Vulnerability Assessment
Derive Test Cases
c
Risk Evaluation Results
Assemble Test Sets
Test Procedure Specification
Security Risk Assessment Artefacts
Derive Test Procedures
d

a) Risk-based identification and prioritization of features sets

b) Risk-based derivation of test conditions and test coverage items

c) Threat scenario based derivation of test cases

d) Risk-based assembly of test procedures

Fraunhofer FOKUS

RASEN
www.rasenproject.eu

ACTIVITIES ARE SPECIFIED IN DETAIL TO PROVIDE GUIDANCE

Identifier

Environment

Pre-and Postconditions

Scenario

I/O

Name	**Risk-based identification and prioritization of features sets (a)**
Actors	Security Tester (ST), Security Risk Analyst (SRA)
Tools	Test Specification Tool (STST), Security Risk Assessment Tool (SRAT)
Precondition	Security relevant features are documented and the security risk assessment is available
Postcondition	Security relevant features to be tested are grouped with respect to potential vulnerabilities and threat scenarios.
Scenario	1. The Security Tester should identify testable security relevant features that need to be covered by security testing. The security tester classifies the security relevant features by grouping them to form feature sets that each addresses exactly one threat scenario and/or one vulnerability. 2. The Security Tester should prioritize the security relevant feature sets using the risk levels that are associated with the threat scenario and/or vulnerabilities. 3. The Security Tester should document the relations between security relevant feature sets and their associated threat scenarios and/or vulnerabilities (maintain traceability).
Data exchanged/ processed	**In:** *Vulnerabilities, threat scenarios, unwanted incident, likelihoods, consequences, risk level* **Out:** *Prioritized list of testable security relevant features (security feature sets).*

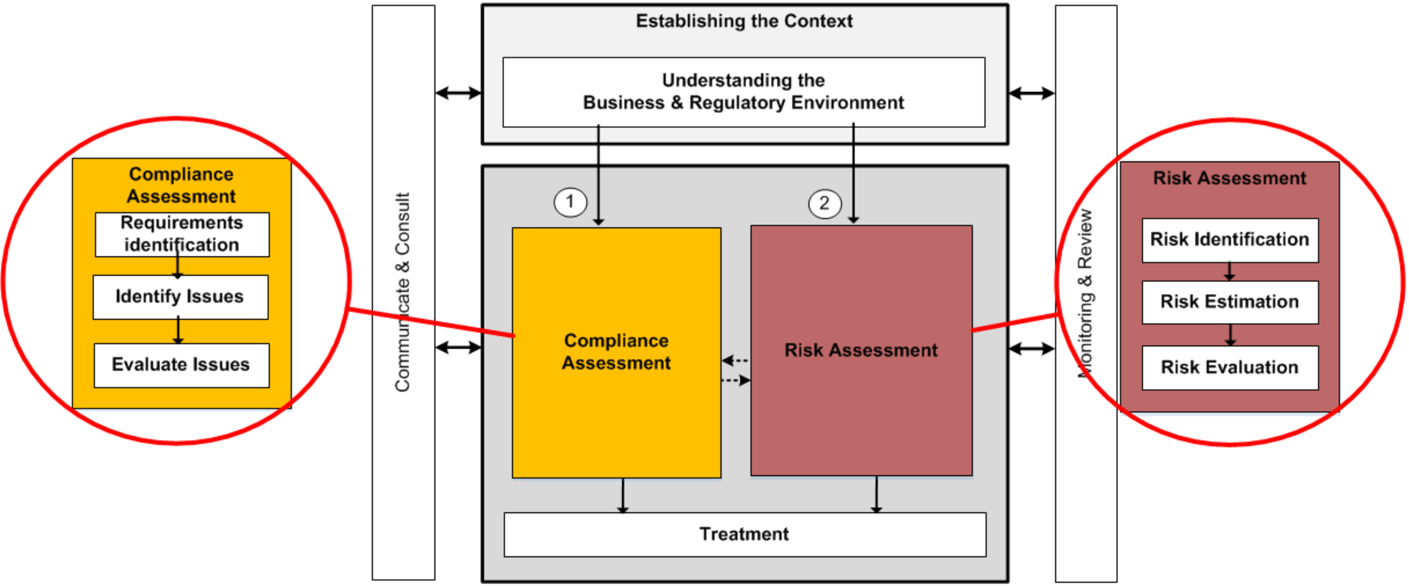
Risk based compliance assessment

Engineering a Connected World

Fraunhofer
FOKUS

RISK AND COMPLIANCE ASSESSMENT

Integrating compliances assessment with security risk assessment



WHY RISK-BASED COMPLIANCE?

Facilitate decisions related to compliance in a risk perspective

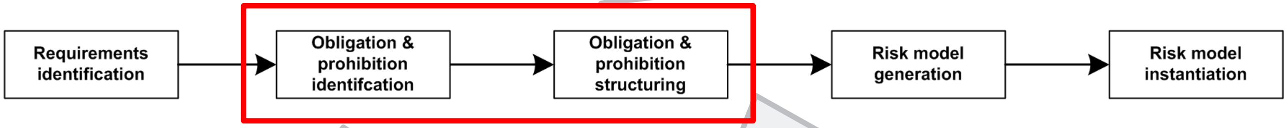
- Security risk assessment takes account of legal and compliance issues.
- Legal risk analysis might help to prioritize the treatment of security risks.
- Security risks can be used as an input for legal risk assessment and support a systematic approach to legal compliance.
- The security risk assessment provides information relevant for compliance with breach notification requirements

1. **Compliance risk identification:** deal with compliance requirements that imply risk
2. **Compliance risk estimation:** understand the underlying uncertainty that might originate in compliance requirements
3. **Compliance risk evaluation:** prioritize compliance requirements based on their level of risk
4. **Treatment:** allocate compliance resources efficiently based on their risk level

CLOSING GAP NORMATIVE STATEMENTS & RISK MODELS

Structured approach

Natural language pattern handling **prohibition** and **obligations**


Requirements identification
Obligation & prohibition identifcation
Obligation & prohibition structuring
Risk model generation
Risk model instantiation

Basic activity pattern

- Compliance norm (obligation, prohibition…)
- Subject-Verb-Object (SVO) sentence structure
  - Subject -> actor (who)
  - Verb -> actions (do-what)
  - Object -> target of action (on-whom)

Modality pattern

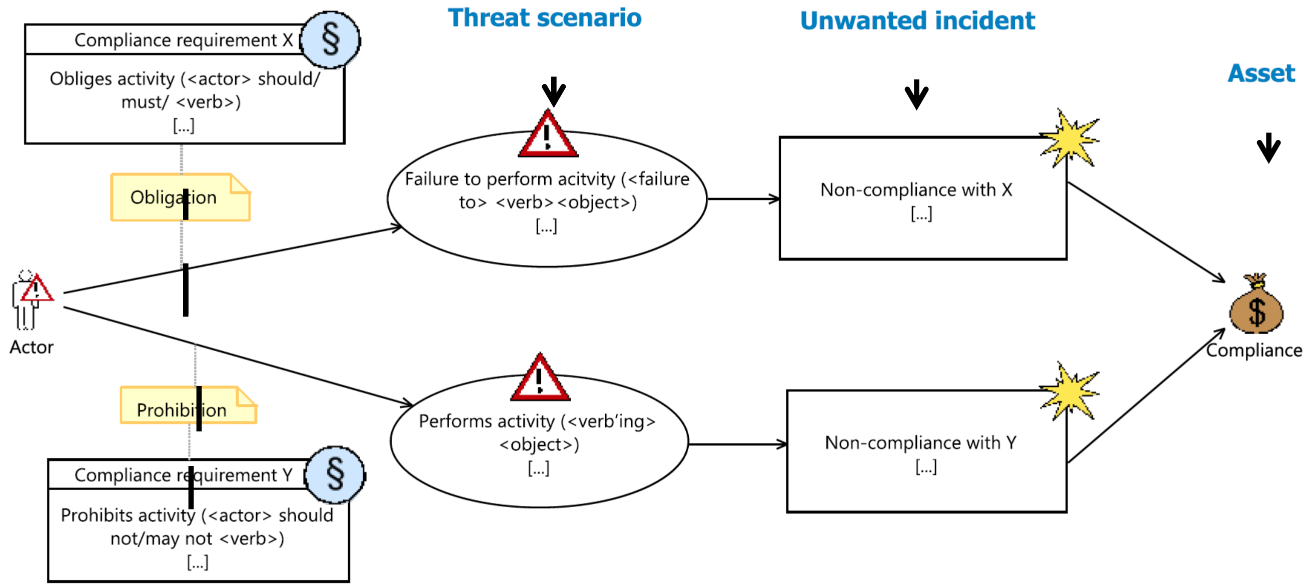
- Use of modal verbs (Eg. shall, must, shall not)
- Patterns for obligation
  - <actor> should <verb> …
  - <actor> must/must be <verb'ed>
- Patterns for prohibition
  - <actor> may not <verb>
  - <actor> shall not> <verb>;

Template for structuring

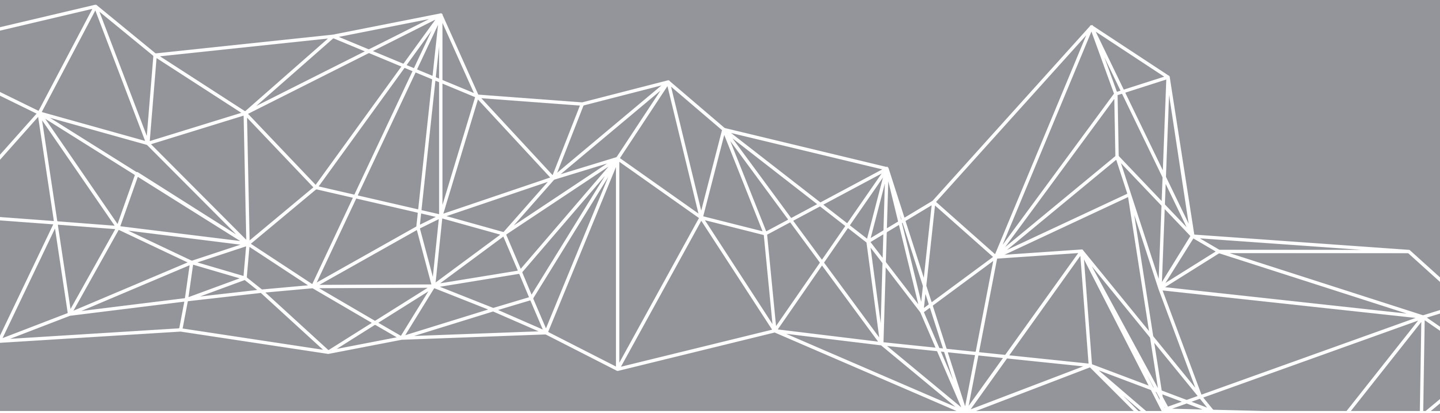
Requirement	Name and/or year, Section/Article number
Modality	Obligation: <actor> ***should/must/*** <verb> or Prohibition: <actor> ***should not/may not*** <verb>
Actor	Subject
Activity	Obligation: <actor> should/must/ <***verb***> Prohibition: <actor> should not/may not <***verb***>
Target	<actor> … <verb> <***object***>
Threat scenario	Contravene obligation: not do activity (what) *<failure to> <verb><object>* Contravene prohibition: do activity (what) *<verb'ing> <object>*
Unwanted incident	*<Non-compliance with> <source of requirement>*

FOKUS

TEMPLATE-BASED MODELS IN CORAS


Threat scenario
Unwanted incident
Asset
Compliance requirement X
§
Obliges activity (<actor> should/ must/ <verb>)
[...]
Obligation
Failure to perform acitvity (<failure to> <verb><object>)
[...]
Non-compliance with X
[...]
Actor
Compliance
Prohibition
Performs activity (<verb'ing> <object>)
[...]
Non-compliance with Y
[...]
Compliance requirement Y
§
Prohibits activity (<actor> should not/may not <verb>)
[...]

SYSTEMATICALLY INTEGRATE BUSINESS-LEVEL RISK ANALYSIS WITH IT-SECURITY RISK ANALYSIS

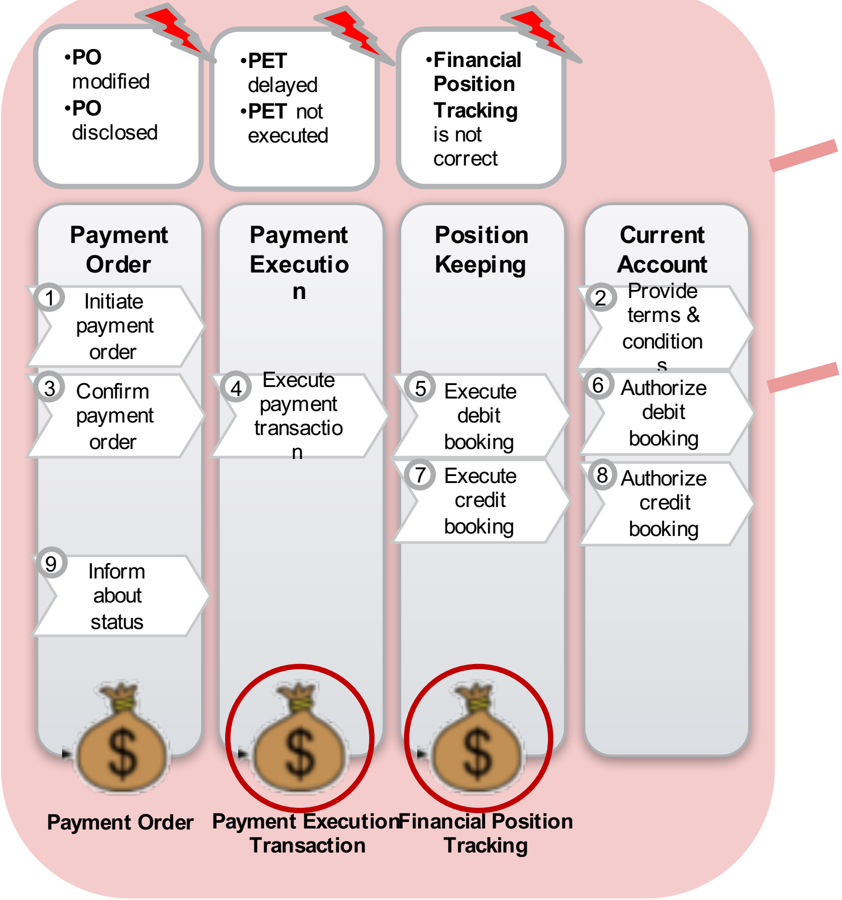


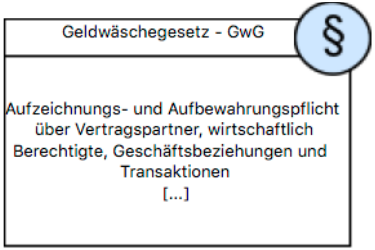
The PREVENT Project

Engineering a Connected World

Fraunhofer
FOKUS

PREVENT: MODEL BUSINESS SCENARIOS AND ASSETS




Geldwäschegesetz - GwG §

Aufzeichnungs- und Aufbewahrungspflicht über Vertragspartner, wirtschaftlich Berechtigte, Geschäftsbeziehungen und Transaktionen
[...]

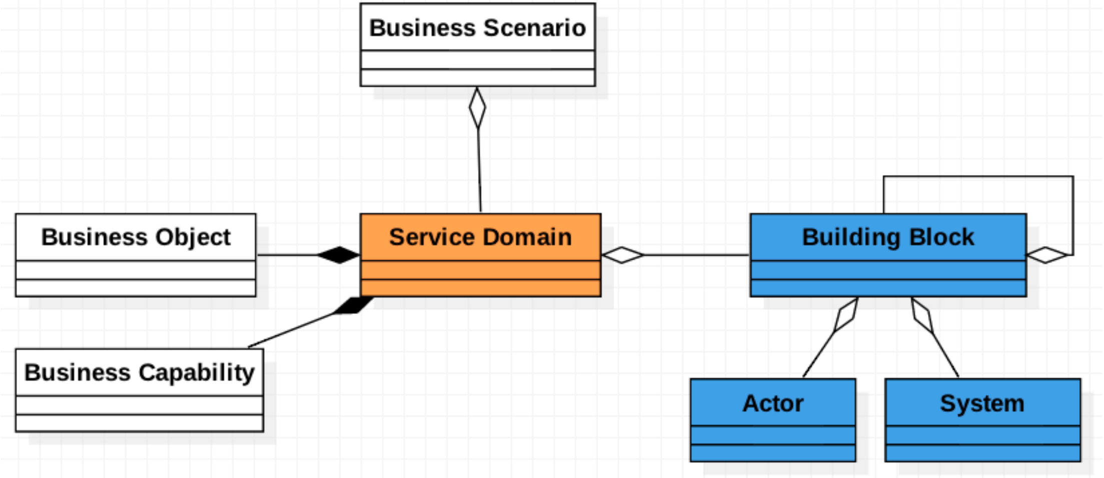
Risk relvant business figures

- Payment: 500.000 transactions/day
- Payment: Payment Order ~5000 Euro

MODEL BUSINESS SCENARIOS AND ASSETS

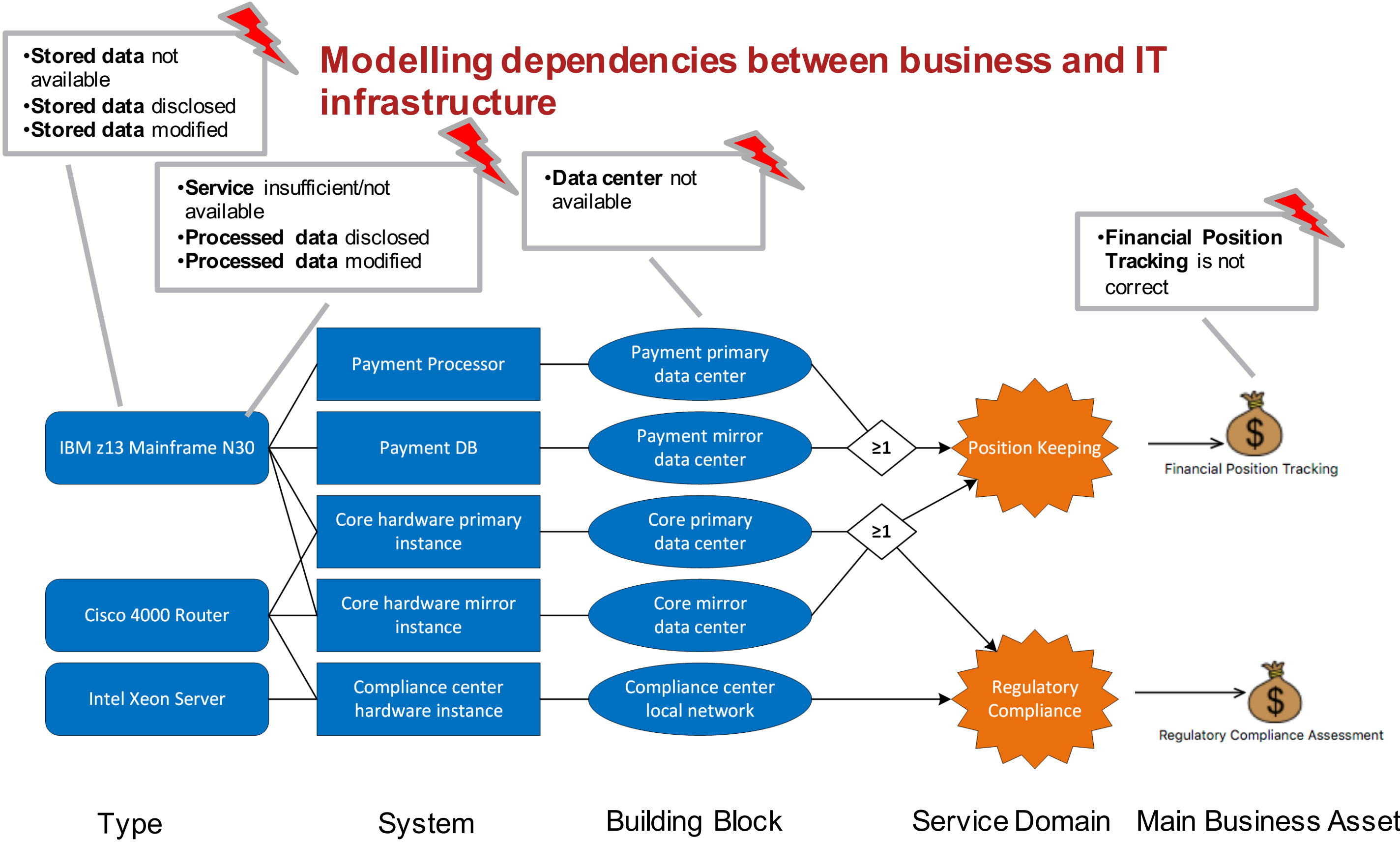
Partitioning the service environment

- „Service Domain“ as starting point for business-level security risk assessment
  - Aggregates to business scenarios
  - Interfaces with IT infrastructure und personell
  - Is used for identification of „Assets“ und „Unwanted Incidents“



MODEL BUSINESS SCENARIOS AND ASSETS

Modelling dependencies between business and IT infrastructure



- **Stored data** not available
- **Stored data** disclosed
- **Stored data** modified

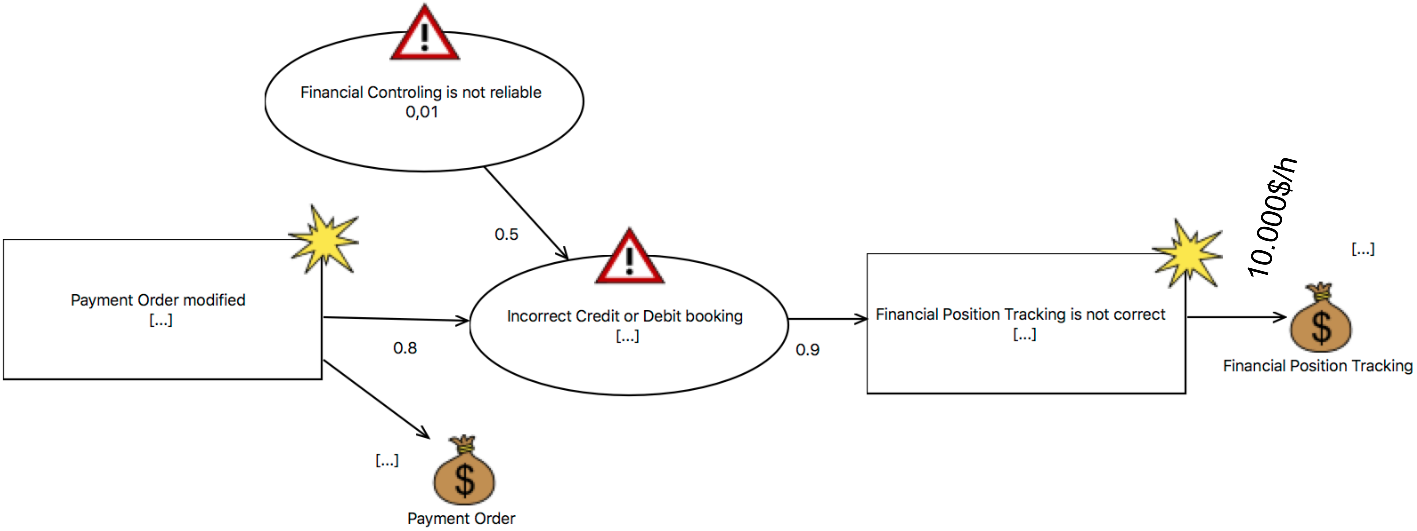
- **Service** insufficient/not available
- **Processed data** disclosed
- **Processed data** modified

- **Data center** not available

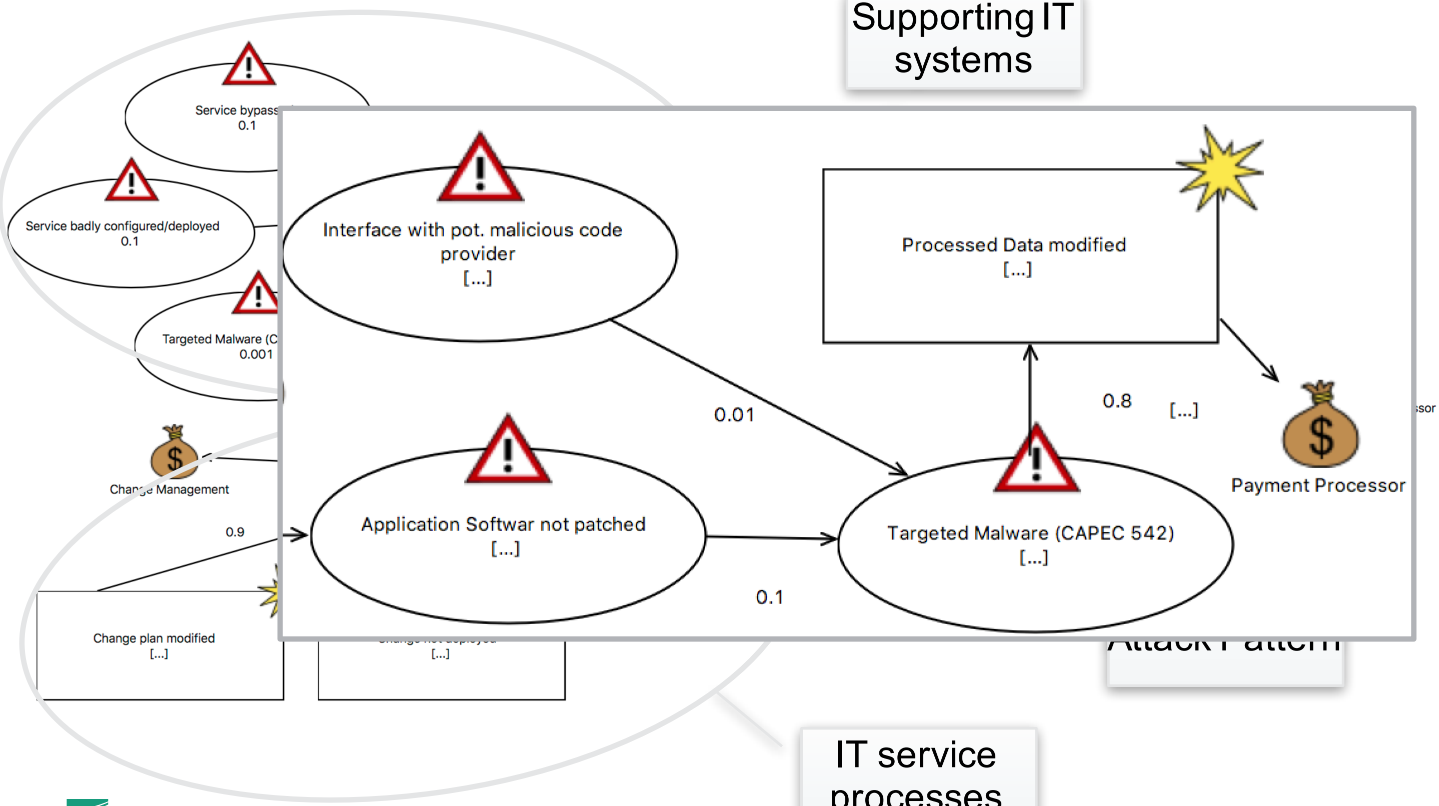
- **Financial Position Tracking** is not correct

IBM z13 Mainframe N30
Cisco 4000 Router
Intel Xeon Server
Payment Processor
Payment DB
Core hardware primary instance
Core hardware mirror instance
Compliance center hardware instance
Payment primary data center
Payment mirror data center
Core primary data center
Core mirror data center
Compliance center local network
≥1
≥1
Position Keeping
Regulatory Compliance
$
Financial Position Tracking
$
Regulatory Compliance Assessment
Type
System
Building Block
Service Domain
Main Business Asset

IDENTIFY UNWANTED INCIDENTS AND THREATS


Financial Controling is not reliable
0,01
0.5
Payment Order modified
[...]
0.8
Incorrect Credit or Debit booking
[...]
0.9
Financial Position Tracking is not correct
[...]
10.000$/h
[...]
Financial Position Tracking
[...]
Payment Order

ANALYSIS OF TECHNICAL INFRASTRUCTURE



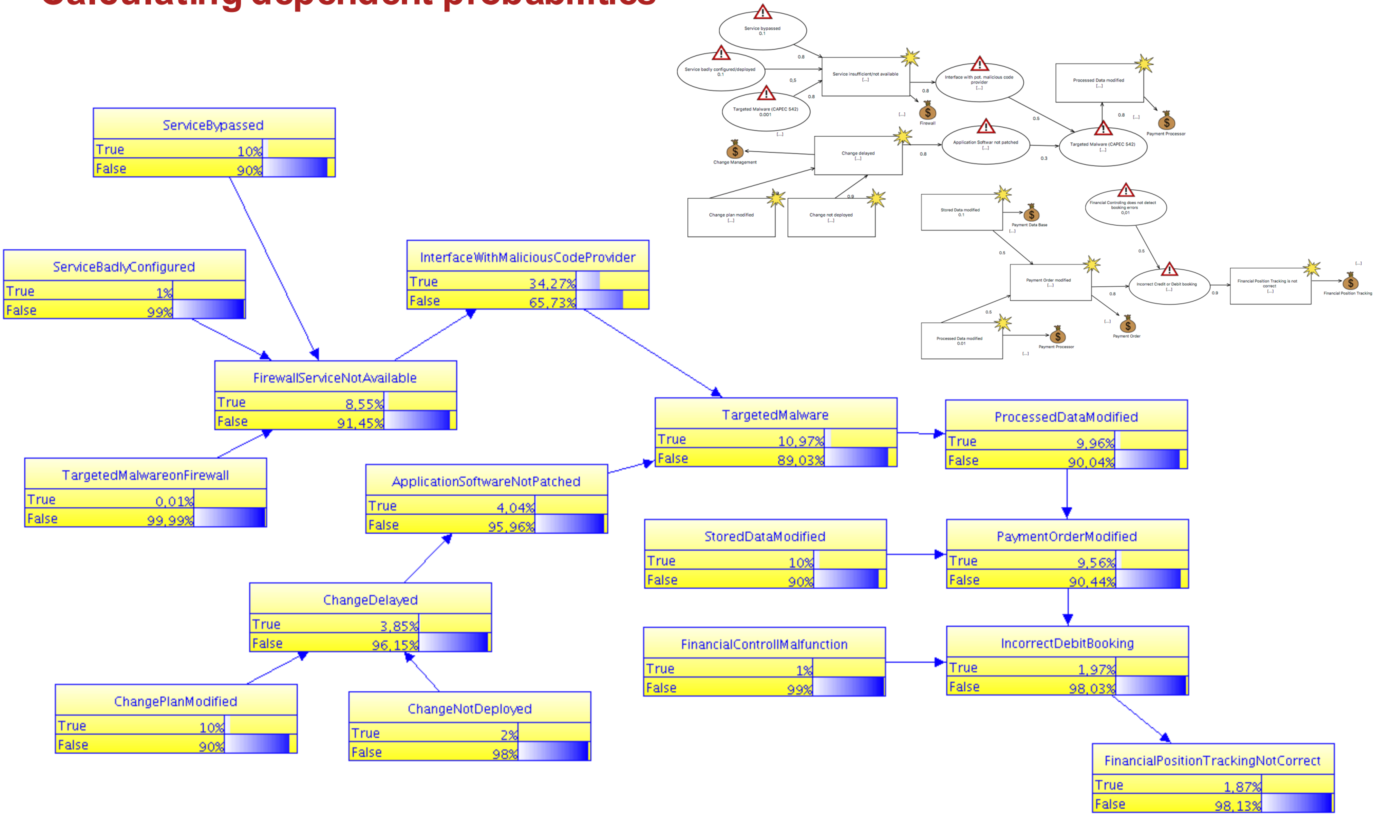
Supporting IT systems

Attack Pattern

IT service processes

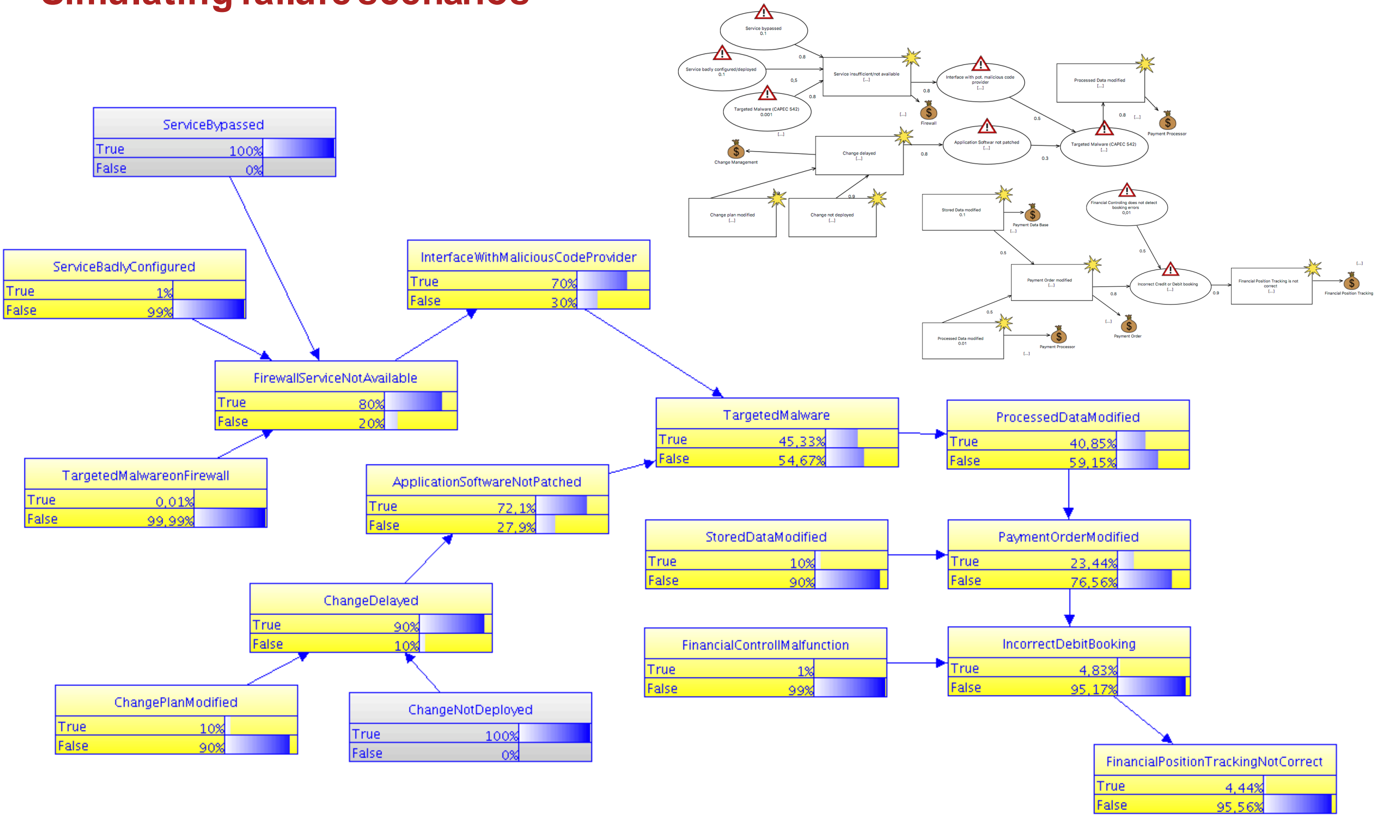
RISK EVALUATION

Calculating dependent probabilities



RISK EVALUATION

Simulating failure scenarios



ServiceBypassed	
True	100%
False	0%

ServiceBadlyConfigured	
True	1%
False	99%

InterfaceWithMaliciousCodeProvider	
True	70%
False	30%

FirewallServiceNotAvailable	
True	80%
False	20%

TargetedMalwareonFirewall	
True	0,01%
False	99,99%

TargetedMalware	
True	45,33%
False	54,67%

ProcessedDataModified	
True	40,85%
False	59,15%

ApplicationSoftwareNotPatched	
True	72,1%
False	27,9%

StoredDataModified	
True	10%
False	90%

PaymentOrderModified	
True	23,44%
False	76,56%

ChangeDelayed	
True	90%
False	10%

FinancialControllMalfunction	
True	1%
False	99%

IncorrectDebitBooking	
True	4,83%
False	95,17%

ChangePlanModified	
True	10%
False	90%

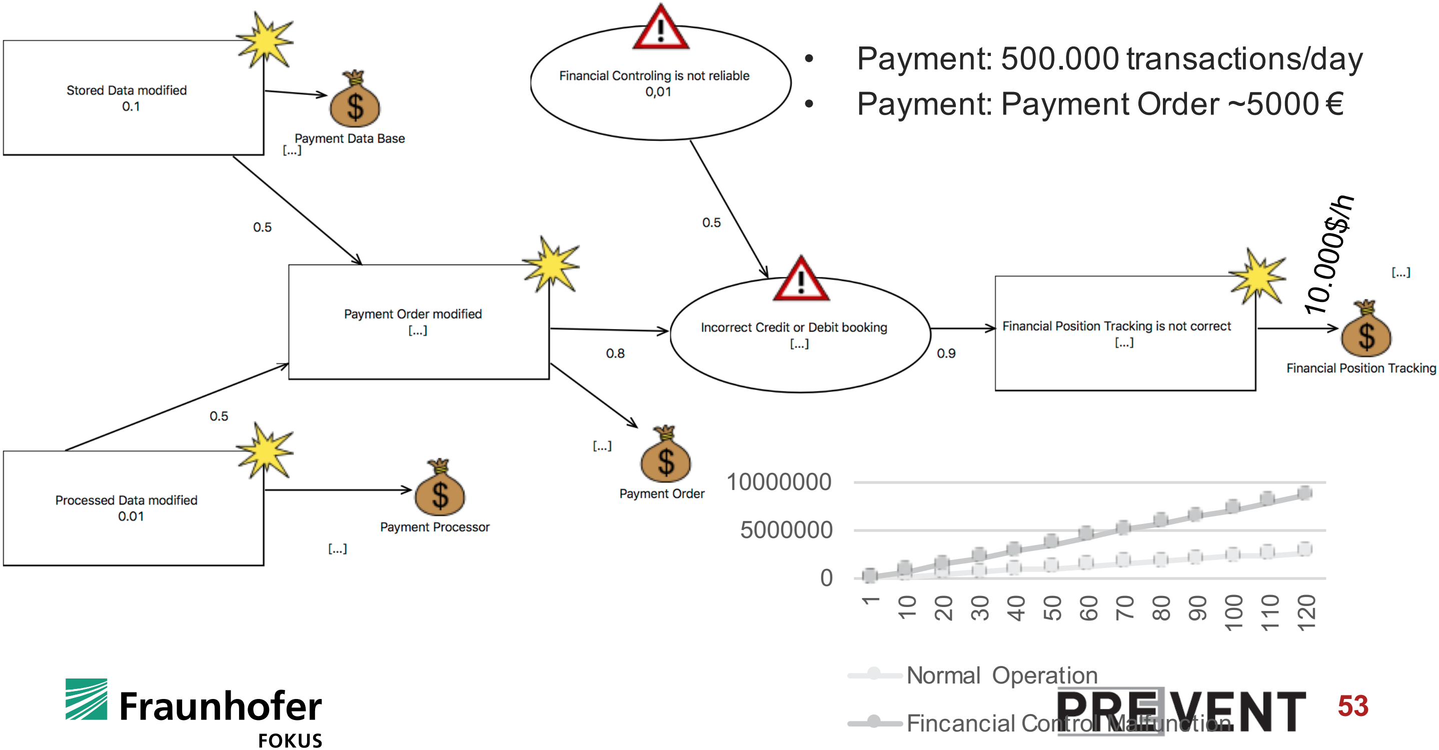
ChangeNotDeployed	
True	100%
False	0%

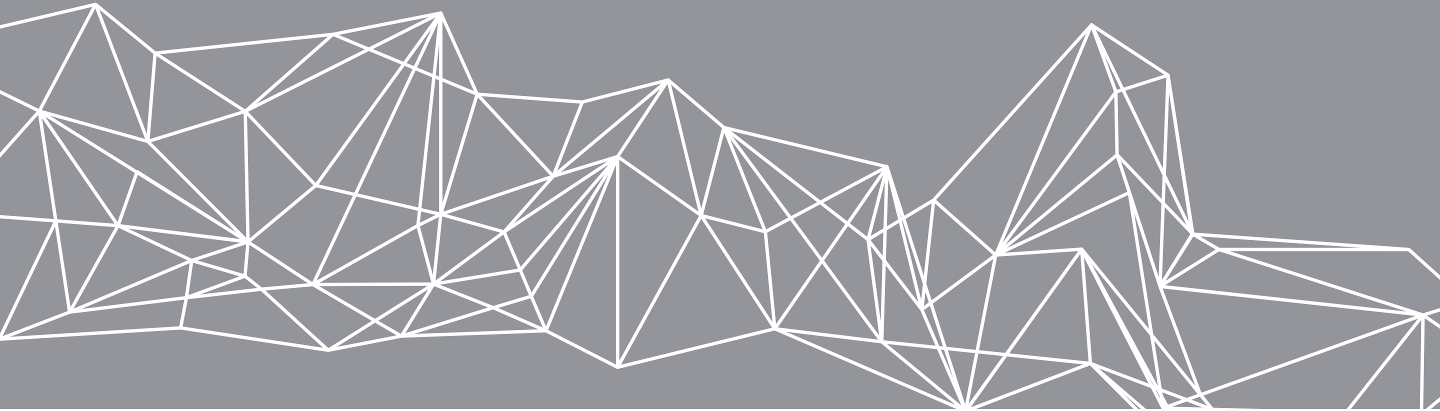
FinancialPositionTrackingNotCorrect	
True	4,44%
False	95,56%

RISK EVALUATION

Evaluation in the context of the business scenario

- Payment: 500.000 transactions/day
- Payment: Payment Order ~5000 €



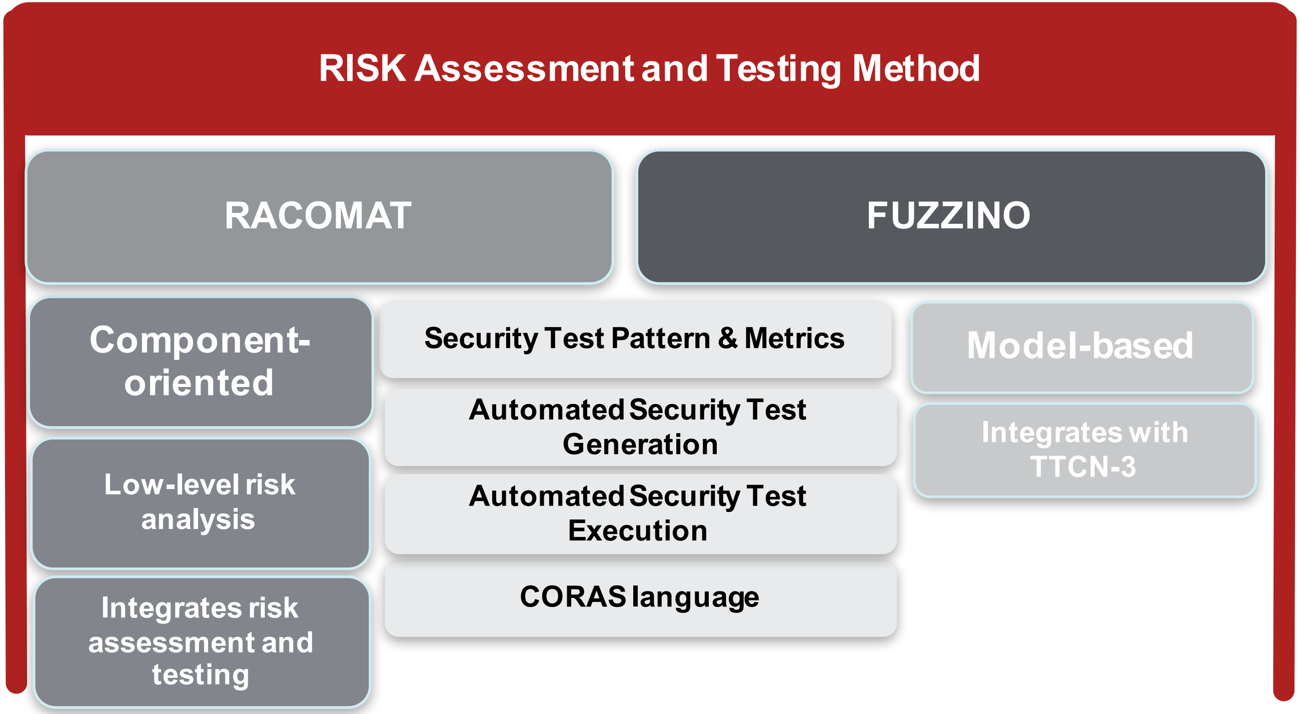


Evaluation, Standardization & Tools

Engineering a Connected World

Fraunhofer
FOKUS

FRAUNHOFER SECURITY TESTING TECHNOLOGY STACK



RISK Assessment and Testing Method

RACOMAT

FUZZINO

Component-oriented

Low-level risk analysis

Integrates risk assessment and testing

Security Test Pattern & Metrics

Automated Security Test Generation

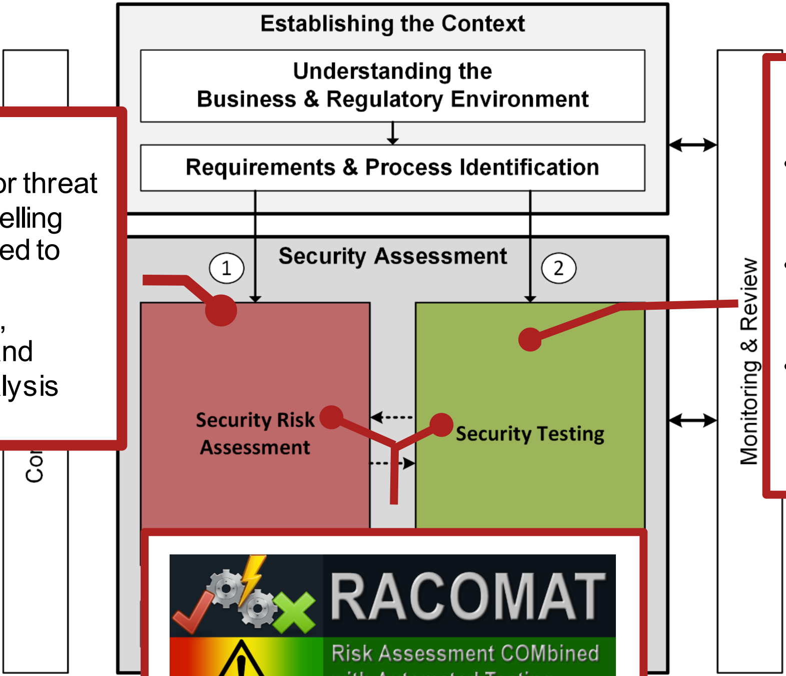
Automated Security Test Execution

CORAS language

Model-based

Integrates with TTCN-3

ADVANCED TOOL SUPPORT



CORAS

- A language for threat and risk modelling
- A tool designed to support documenting, maintaining and reporting analysis results

FUZZINO

- A library that provides generation of test data for fuzz testing
- injecting invalid or unexpected input data to the SUT.
- Support to find security-related weaknesses in your code.

RACOMAT

Risk Assessment COMbined with Automated Testing

- A language and tool to support risk-based security testing

FUZZING

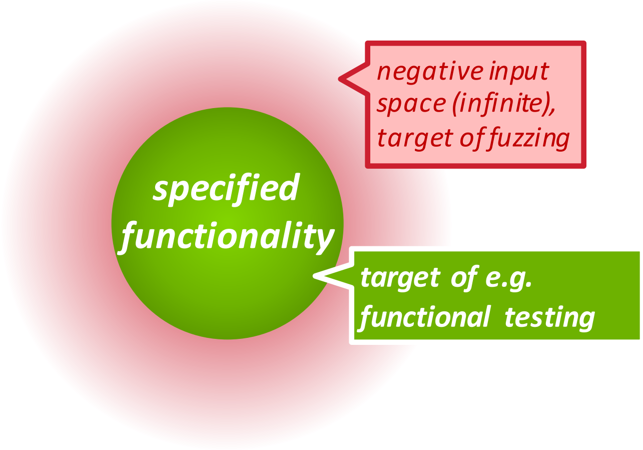
Introduction

- Fuzzing is about **injecting invalid or unexpected inputs**
  - to obtain **unexpected behaviour**
  - to identify **errors** and potential **vulnerabilities**

- Interface robustness testing

- Fuzzing is able **to find (0day-) vulnerabilities**, e.g.
  - crashes
  - denial of service
  - security exposures
  - performance degradation

- highly-automated black box approach

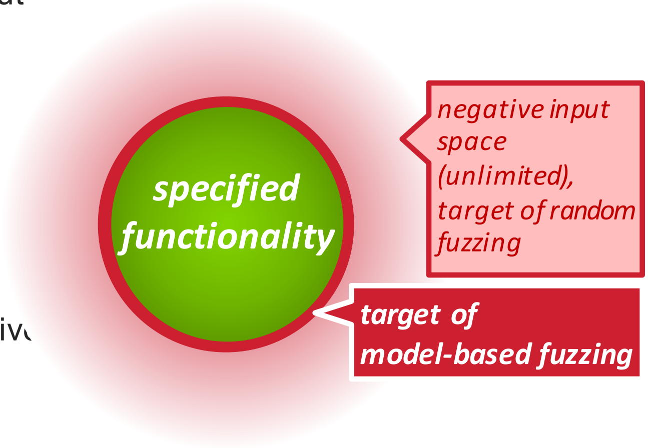

specified functionality
negative input space (infinite), target of fuzzing
target of e.g. functional testing

see also: Takanen, A., DeMott, J., Miller, C.: Fuzzing for Software Security Testing and Quality Assurance. Artech House, Boston (2008)

MODEL-BASED FUZZING

Model-Based Fuzzers

- **Model-based fuzzers** uses models of the input domain (protocol models, e.g. context free grammars), for generating systematic non-random test cases
- The model is used to generate complex interaction with the SUT.
- Employ fuzzing heuristics to reduce the negativ input space
- Model-based fuzzers finds defects which human testers would fail to find.


specified functionality
negative input space (unlimited), target of random fuzzing
target of model-based fuzzing

see also: Takanen, A., DeMott, J., Miller, C.: Fuzzing for Software Security Testing and Quality Assurance. Artech House, Boston (2008)

Fraunhofer FOKUS

MODEL-BASED FUZZING

Fuzzing Library Fuzzino

- make traditional data **fuzzing widely available**
  - allow an **easy integration into existing tools**
  - **without deep knowledge** about fuzz data generation

- allow data fuzzing **without the need for**
  - **making familiar** with a specific fuzzing tool
  - **integrating further fuzzing tools** into the test process

- approach: didn’t reinvent the wheel, **used the potential of existing fuzzing tools**

Peach

Sulley

MODEL-BASED FUZZING

Fuzzing Library Fuzzino: Advantages

FUZZINO

- allows **generation and mutation based fuzzing**

- **platform independent**: the library is implemented on **Java** running on many platforms
- **language independent**: the library provides an **XML**-based interface

- **automated**: Fuzzino automatically selects appropriate fuzzing heuristics
- **communicative**: Fuzzino tells you which fuzzing heuristics are used

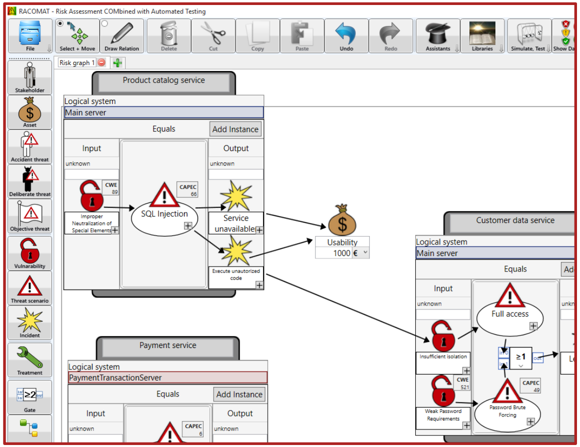
- efficient: the user can decide
  - **which fuzzing heuristics** shall be used
  - **amount of fuzz test data**: avoids generating billions of values

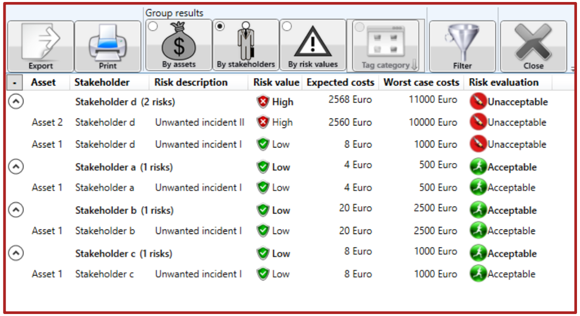
- further extensions support grammars and regular expressions

FRAUNHOFER RACOMAT

A toolset for Risk Assessment and Automated Testing

- Tool developed by Fraunhofer FOKUS within the RASEN project
- Assisted, literature based risk assessment
- Compositional risk assessment with incident simulation
- Risk based security testing
- Test based risk assessment
- Dashboard risk evaluation results to support the management
- Stand alone tool and Visual Studio plug-in
- Integration platform for other tools



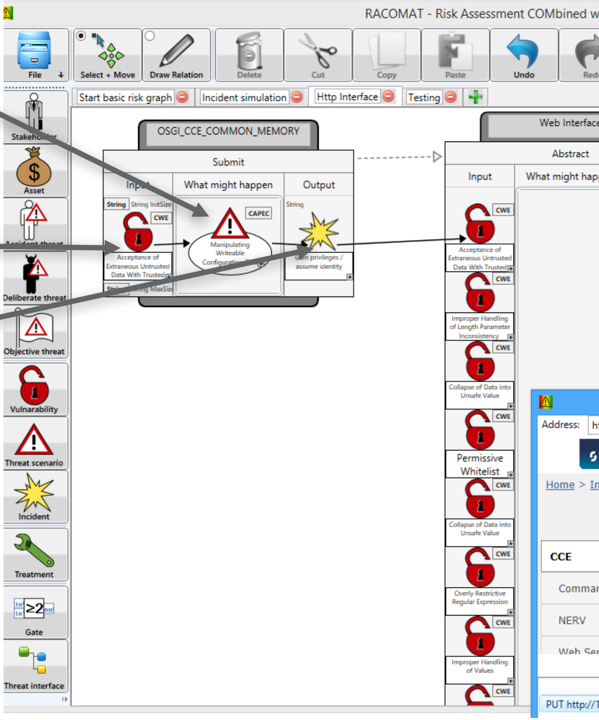


-	Asset	Stakeholder	Risk description	Risk value	Expected costs	Worst case costs	Risk evaluation
⌃		Stakeholder d (2 risks)		High	2568 Euro	11000 Euro	Unacceptable
	Asset 2	Stakeholder d	Unwanted incident II	High	2560 Euro	10000 Euro	Unacceptable
	Asset 1	Stakeholder d	Unwanted incident I	Low	8 Euro	1000 Euro	Unacceptable
⌃		Stakeholder a (1 risks)		Low	4 Euro	500 Euro	Acceptable
	Asset 1	Stakeholder a	Unwanted incident I	Low	4 Euro	500 Euro	Acceptable
⌃		Stakeholder b (1 risks)		Low	20 Euro	2500 Euro	Acceptable
	Asset 1	Stakeholder b	Unwanted incident I	Low	20 Euro	2500 Euro	Acceptable
⌃		Stakeholder c (1 risks)		Low	8 Euro	1000 Euro	Acceptable
	Asset 1	Stakeholder c	Unwanted incident I	Low	8 Euro	1000 Euro	Acceptable

Fraunhofer
FOKUS

AUTOMATED RISK-BASED SECURITY TESTING WITH RACOMAT

- RACOMAT uses the combined system and risk model to instantiate test patterns
  - Attack patterns indicate which test patterns should be used
    - Priority of tests can be calculated based on likelihood and consequence values
  - Vulnerabilities indicate where to stimulate the SUT
  - Unwanted Incidents can be introduced in order to determine what should be observed to get some verdict
  - ➢ **Complete automation often achievable**
  - Implementing generic reusable test pattern is challenging
  - Currently not really saving manual effort
  - ➢ **Vision: open security test pattern library**



EVALUATION

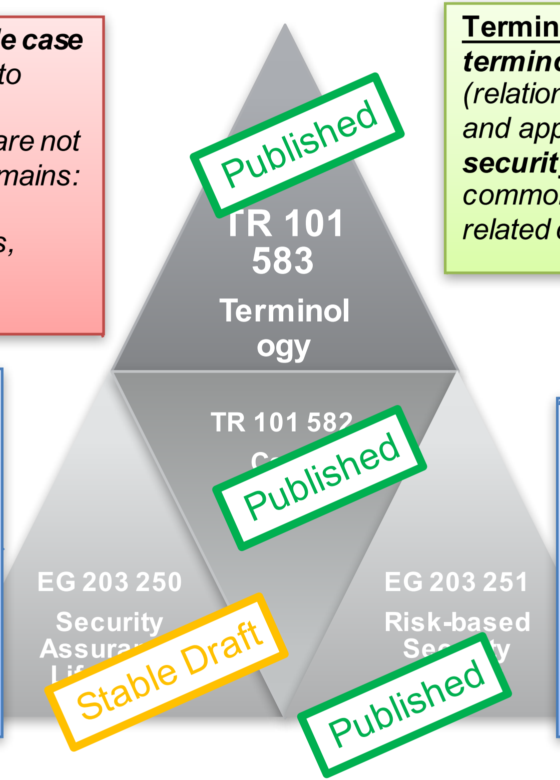
Case studies from recent research projects

- Money counting machine (DIAMONDS project with Giesecke Devrient)
- Automotive mullti media device (DIAMONDS project with Dornier Consulting)
- Business software development (RASEN project with Software AG)
- Banking data centers (PREVENT project with Hypovereinsbank and Wincor Nixdorf)

SECURITY TESTING STANDARDIZATION AT ETSI

Case Studies: *To* ***assemble case study experiences*** *related to security testing. Industrial experiences may cover but are not restricted to the following domains: Smart Cards, Industrial Automation, Radio Protocols, Transport/Automotive, Telecommunication*

Terminology: *To collect the* ***basic terminology and ontology*** *(relationship between stake holder and application)* ***to be used for security testing*** *in order to have a common understanding in MTS and related committees.*



Security Assurance Life Cycle: ***Guidance to*** *the application* ***system designers*** *in such a way to maximise both security assurance and the verification and validation of the capabilities offered by the system's security measures.*

Risk assessment and risk-based security testing methodologies: *Describes a* ***set of methodologies*** *that combine* ***risk assessment and testing****. The methodologies are based on standards like ISO 31000 and IEEE 29119*

SUMMARY

Methods and tools for improved security

- Fraunhofer Security Testing Stack Covers the integration of security testing and risk assessment
- Is concisely specified
- Is mature and powerful
  - applied to several case studies
  - integrates with recent risk assessment and testing standards
  - constitutes standardization work item at ETSI
- Mature tool support available
  - RACOMAT https://www.youtube.com/watch?v=uzxIdtf59QM)
  - FUZZINO https://github.com/fraunhoferfokus/Fuzzino
- Research project to map results to banking and IOT

RISK WORKSHOP OCTOBER 17TH-19TH IN GRAZ

4th International Workshop on Risk Assessment and Risk-driven Quality Assurance (RISK)

- In conjunction with 28th International Conference on Testing Software and Systems (ICTSS)
- **Springer LNCS post proceedings**
- Long paper, short paper and extended abstracts
- Important dates:
  - Submission deadline: **September 18th**
  - Notification of authors: **October 4th**
  - Camera ready paper submission: **February 2017**

- **More information: https://www.fokus.fraunhofer.de/en/events/risk_2016**

CONTACT US IF YOU ARTE INTERESTED

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
www.fokus.fraunhofer.de

Jürgen Großmann
Project Manager
juergen.grossmann@fokus.fraunhofer.de
Phone +49 (0)30 3463-7390