Risk-Based Software Quality and Security Engineering in Data-Intensive Environments

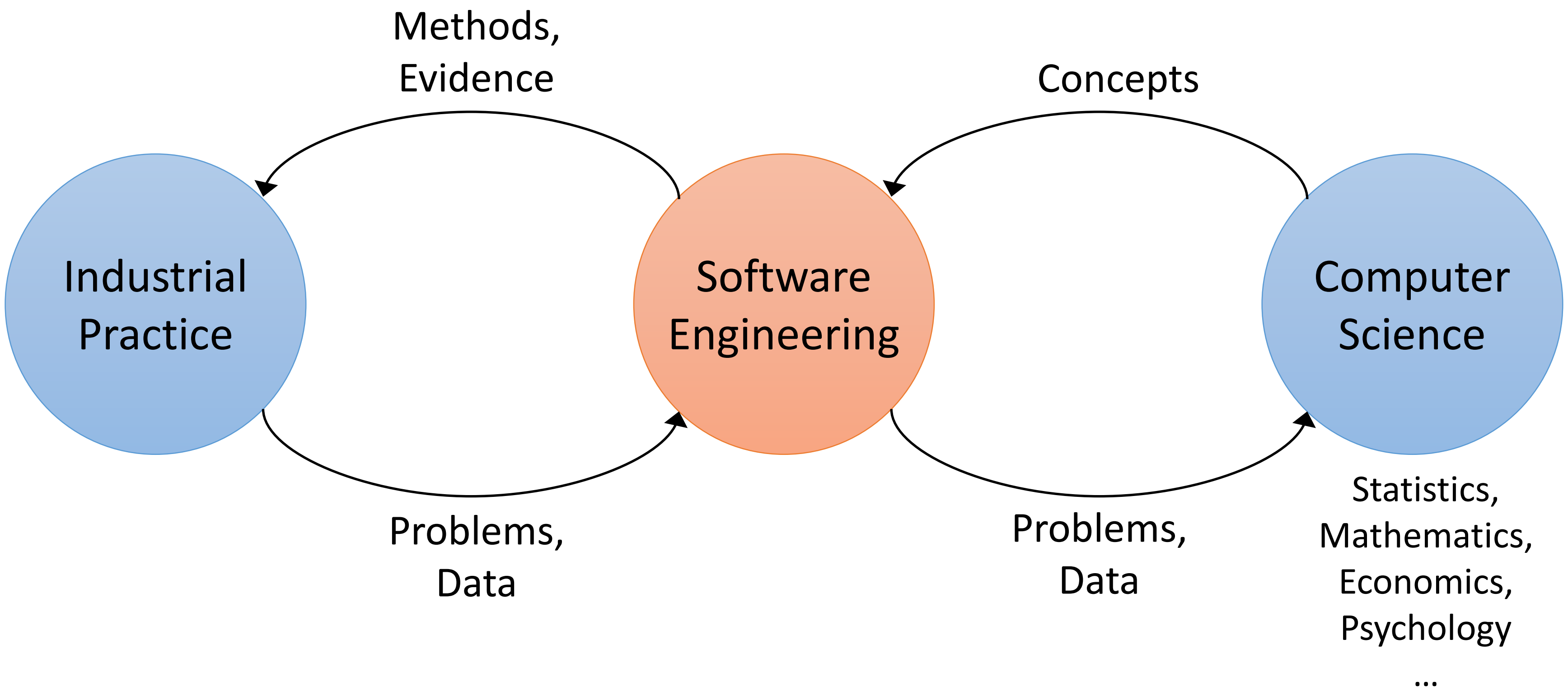
Prof. Dr. Michael Felderer

Department of Computer Science

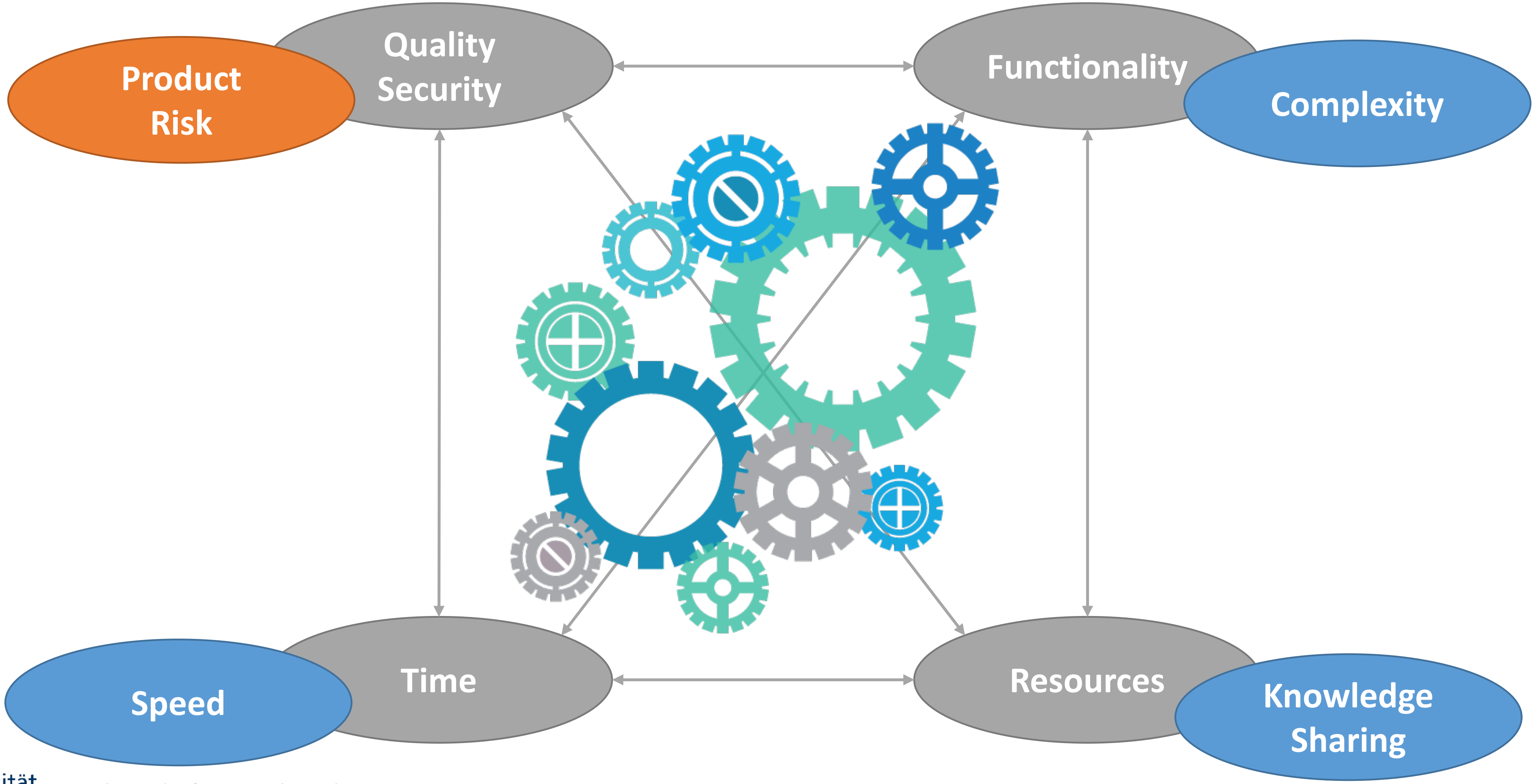
Universität Innsbruck

Austria

Software Engineering As Applied Engineering Science



Quality, Security and Risk in Software Development



Product Risk

Quality Security

Functionality

Complexity

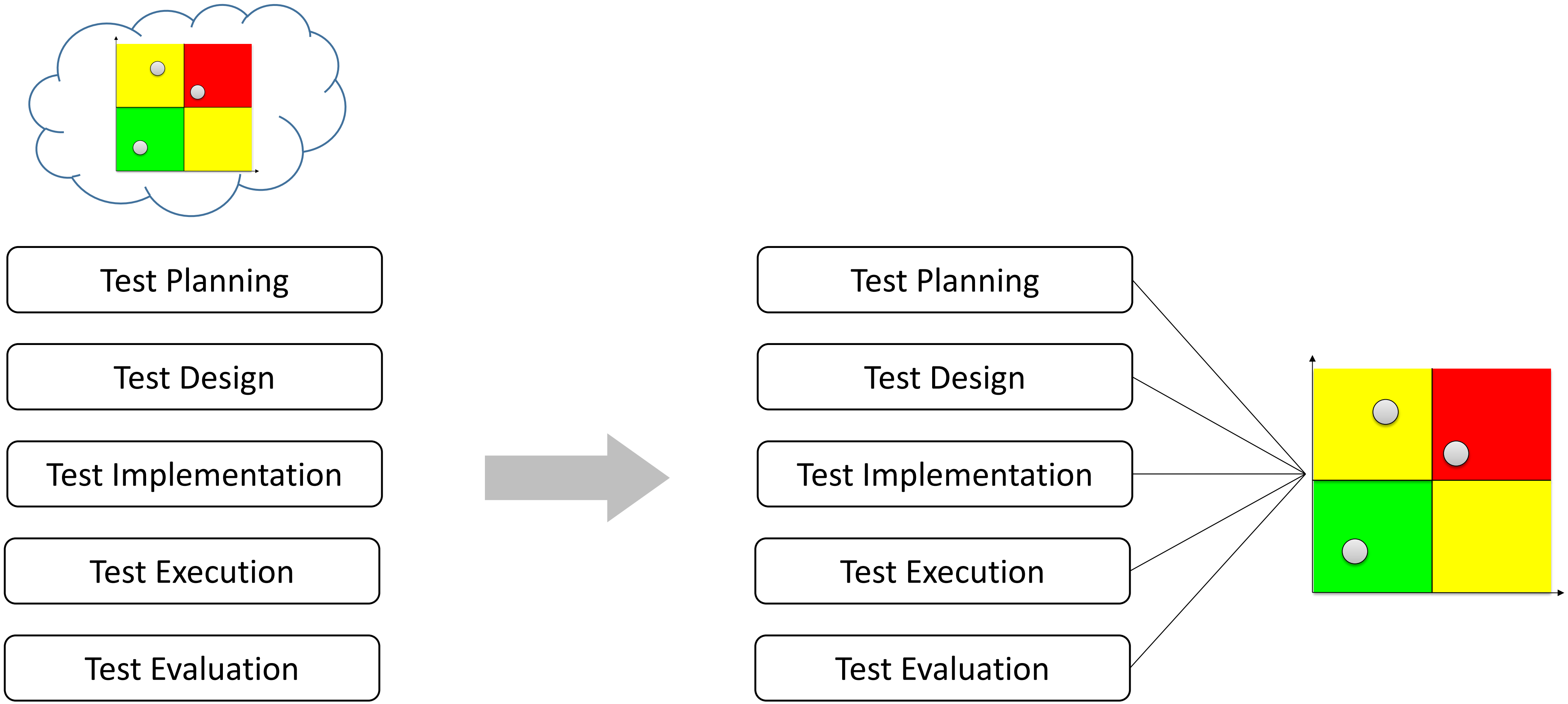
Time

Speed

Resources

Knowledge Sharing

Risk-Based Testing (Risk-Based Quality Assurance)



Test Planning

Test Design

Test Implementation

Test Execution

Test Evaluation

Test Planning

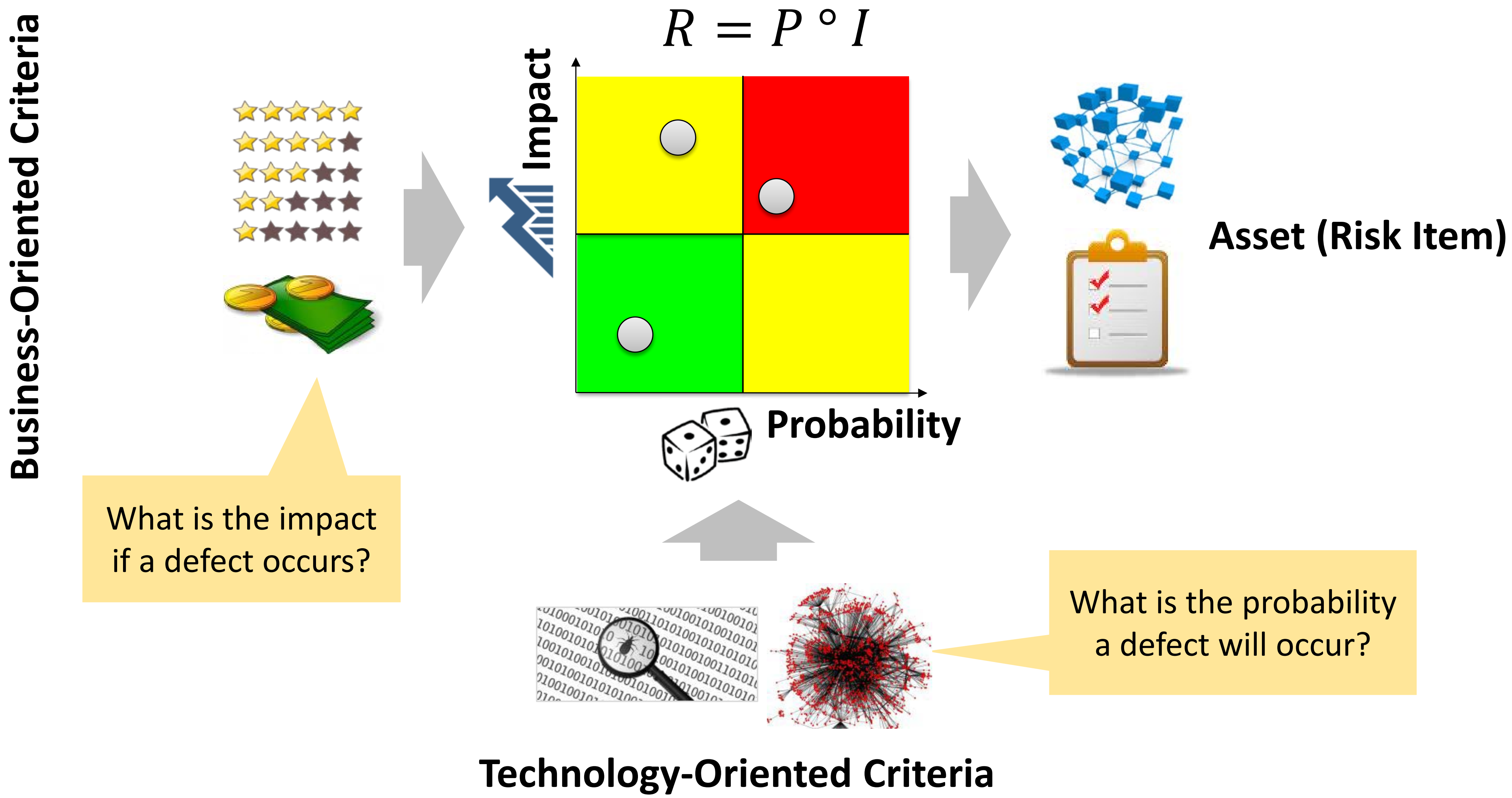
Test Design

Test Implementation

Test Execution

Test Evaluation

Risk Concept in Software Quality Engineering



$$R = P \circ I$$

Impact

Probability

Business-Oriented Criteria

What is the impact if a defect occurs?

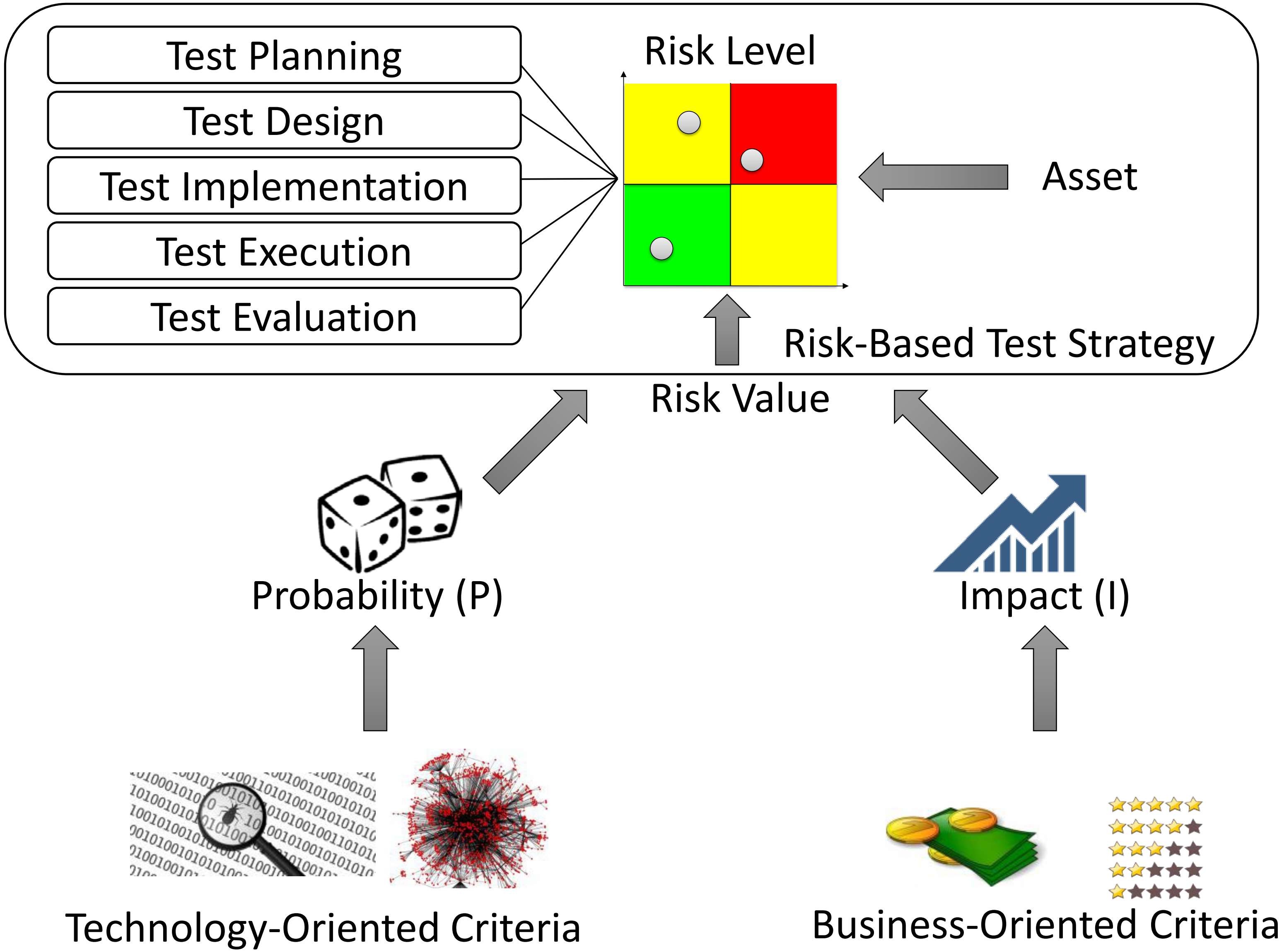
Asset (Risk Item)

What is the probability a defect will occur?

Technology-Oriented Criteria

Risk-Based Test Strategy

Felderer, M., Schieferdecker, I.: *A taxonomy of risk-based testing*. Software Tools for Technology Transfer, 16(5), 559-568, 2014



Test Planning

Test Design

Test Implementation

Test Execution

Test Evaluation

Risk Level

Asset

Risk-Based Test Strategy

Risk Value

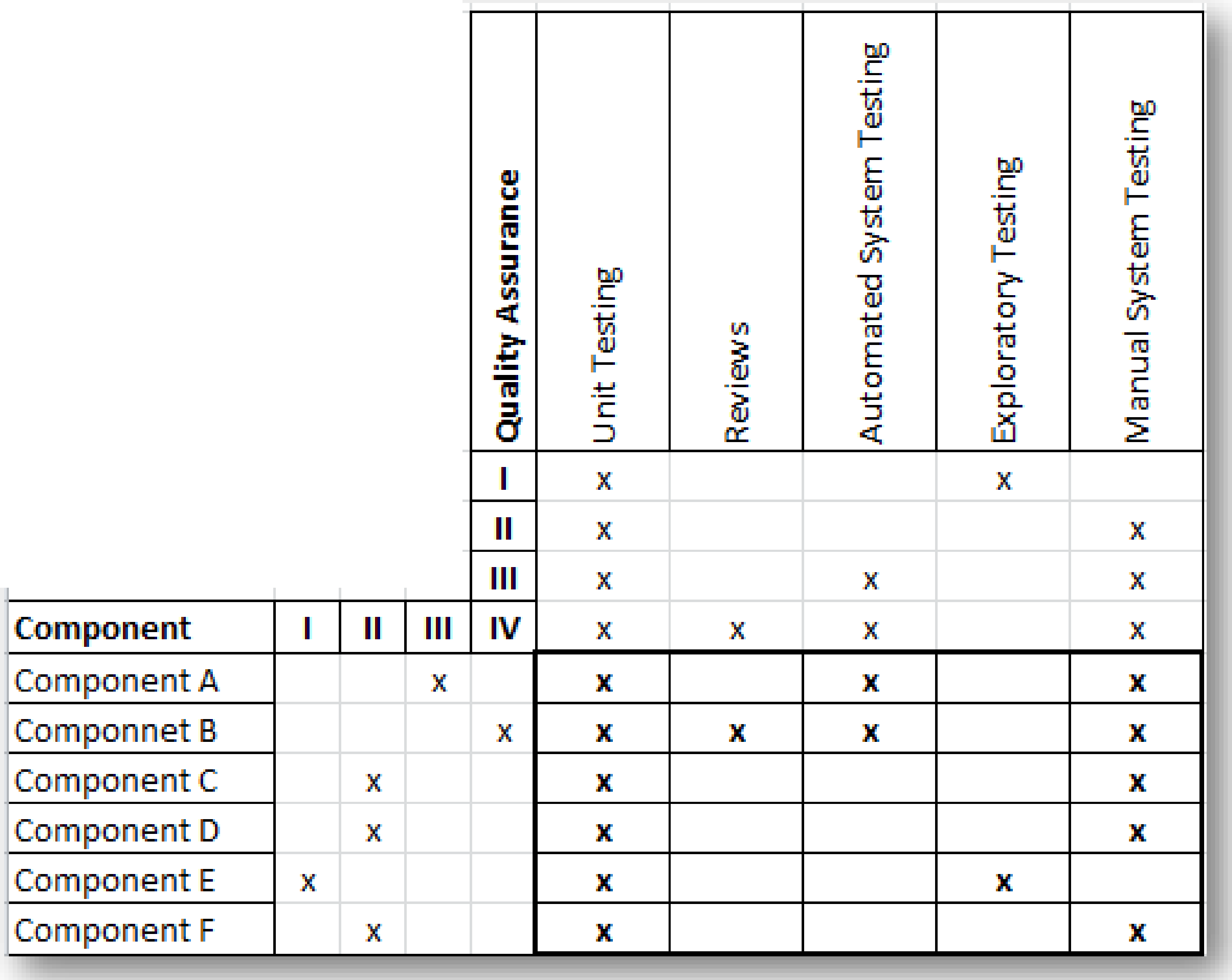
Probability (P)

Impact (I)

Technology-Oriented Criteria

Business-Oriented Criteria

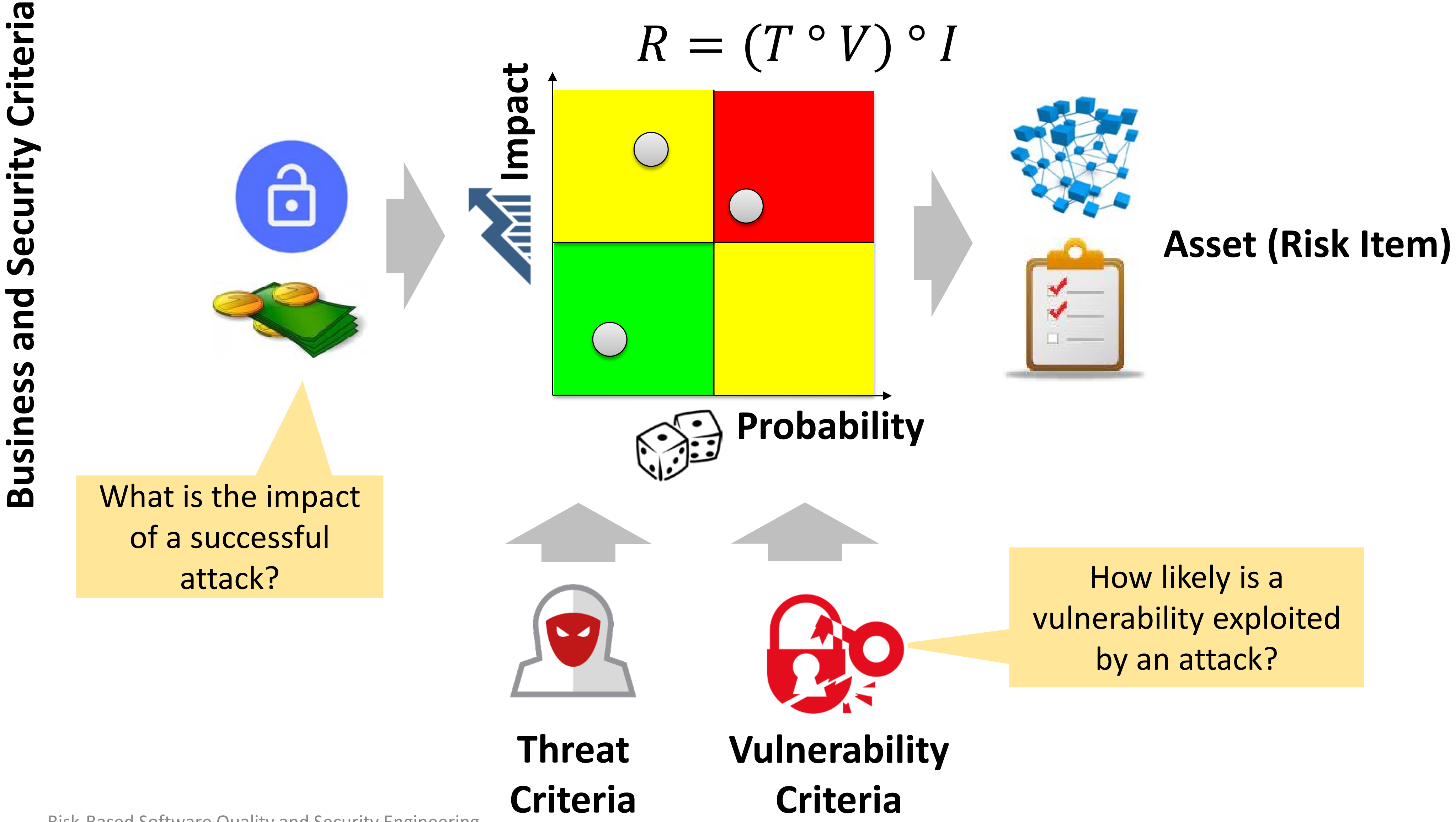
Example of a Risk-Based Test Strategy



Quality Assurance	Unit Testing	Reviews	Automated System Testing	Exploratory Testing	Manual System Testing
I	x			x	
II	x				x
III	x		x		x
IV	x	x	x		x

Component	I	II	III	IV	Unit Testing	Reviews	Automated System Testing	Exploratory Testing	Manual System Testing
Component A			x		**x**		**x**		**x**
Componnet B				x	**x**	**x**	**x**		**x**
Component C		x			**x**				**x**
Component D		x			**x**				**x**
Component E	x				**x**			**x**	
Component F		x			**x**				**x**

Risk Concept in Software Security Engineering



$$R = (T \circ V) \circ I$$

Business and Security Criteria

Impact

Probability

Asset (Risk Item)

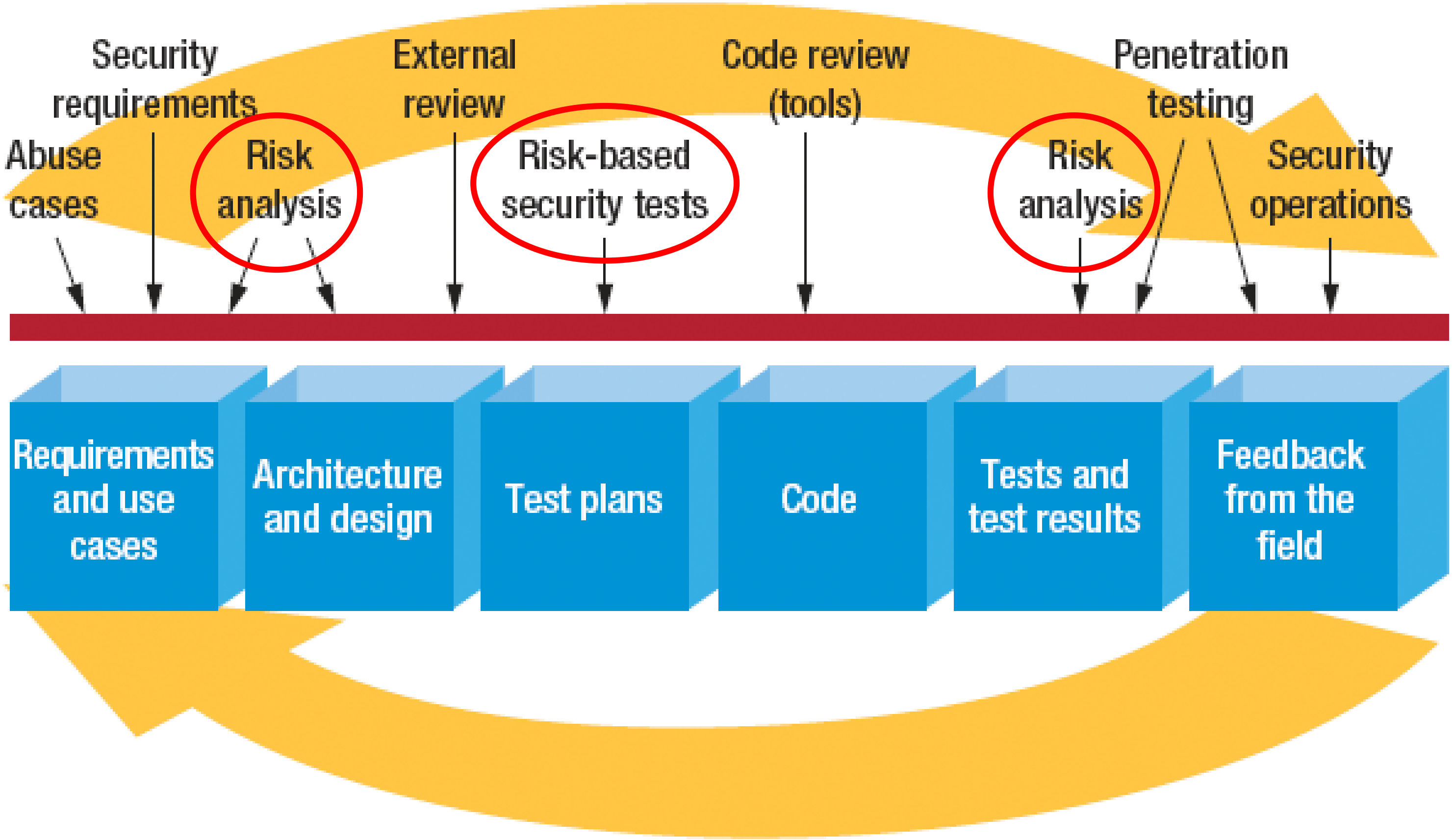
What is the impact of a successful attack?

How likely is a vulnerability exploited by an attack?

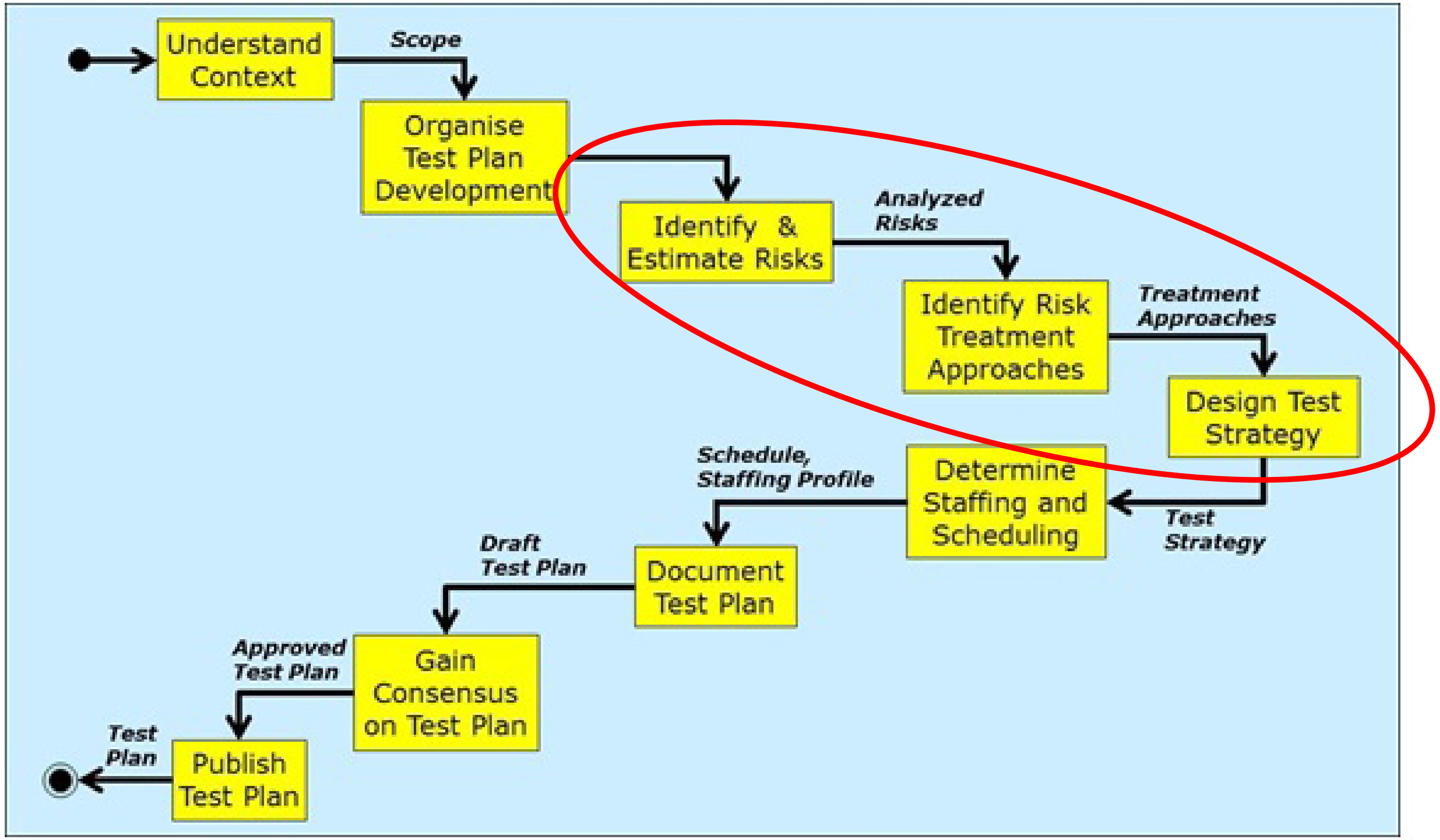
Threat Criteria

Vulnerability Criteria

Security Touchpoints: Risk Concept and Software Security



ISO/IEC/IEEE 29119: Risk Concept and Software Quality


Understand Context
Scope
Organise Test Plan Development
Identify & Estimate Risks
Analyzed Risks
Identify Risk Treatment Approaches
Treatment Approaches
Design Test Strategy
Test Strategy
Determine Staffing and Scheduling
Schedule, Staffing Profile
Document Test Plan
Draft Test Plan
Gain Consensus on Test Plan
Approved Test Plan
Publish Test Plan
Test Plan

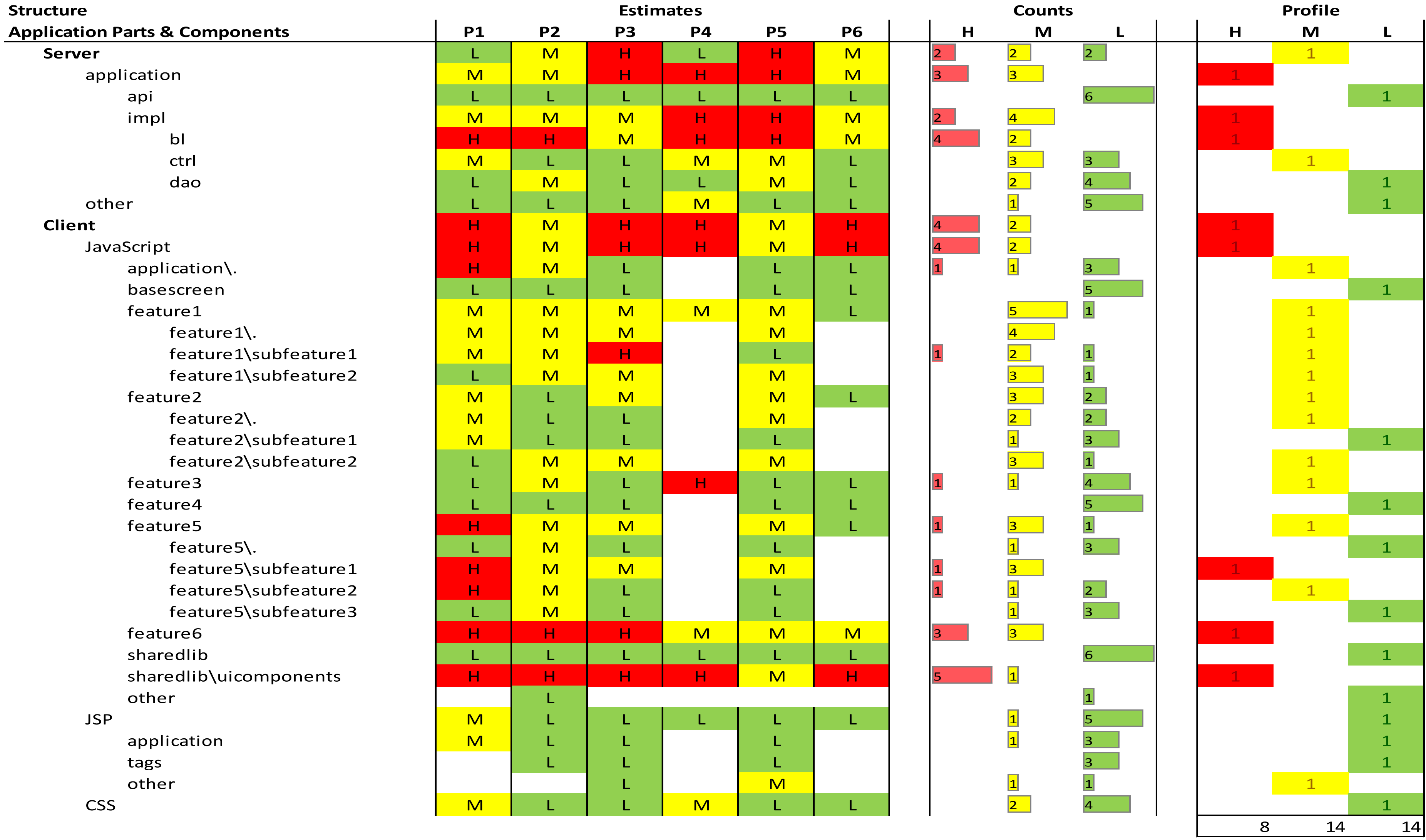
http://softwaretestingstandard.org/

Potential Benefits of Risk-Based Quality Engineering

- **Organizational support** to manage test knowledge
  - Knowledge sharing
  - Improved decision support
  - Compliance to standards
- Improved test **effectiveness** to control complexity
  - Detection of additional defects
  - Earlier detection of critical defects
  - Increased defect detection rate of single tests
- Improved **efficiency** to control speed of testing
  - Reduction of testing time
  - Reduction of testing budget
  - Earlier release date

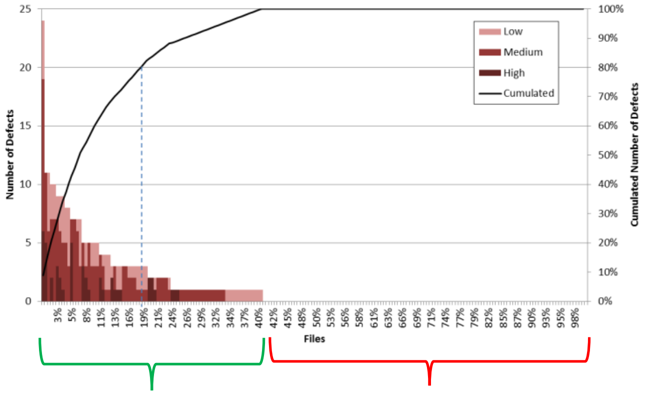
Issues of Introducing Risk-Based Testing

Felderer, M., Ramler, R.: *Integrating risk-based testing in industrial test processes*. Software Quality Journal, 22(3), 543-575, 2014



Structure	**Estimates**						**Counts**			**Profile**		
Application Parts & Components	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**H**	**M**	**L**	**H**	**M**	**L**
Server	L	M	H	L	H	M	2	2	2		1	
application	M	M	H	H	H	M	3	3		1		
api	L	L	L	L	L	L			6			1
impl	M	M	M	H	H	M	2	4		1		
bl	H	H	M	H	H	M	4	2		1		
ctrl	M	L	L	M	M	L		3	3		1	
dao	L	M	L	L	M	L		2	4			1
other	L	L	L	M	L	L		1	5			1
Client	H	M	H	H	M	H	4	2		1		
JavaScript	H	M	H	H	M	H	4	2		1		
application\.	H	M	L		L	L	1	1	3		1	
basescreen	L	L	L		L	L			5			1
feature1	M	M	M	M	M	L		5	1		1	
feature1\.	M	M	M		M			4			1	
feature1\subfeature1	M	M	H		L		1	2	1		1	
feature1\subfeature2	L	M	M		M			3	1		1	
feature2	M	L	M		M	L		3	2		1	
feature2\.	M	L	L		M			2	2		1	
feature2\subfeature1	M	L	L		L			1	3			1
feature2\subfeature2	L	M	M		M			3	1		1	
feature3	L	M	L	H	L	L	1	1	4		1	
feature4	L	L	L		L	L			5			1
feature5	H	M	M		M	L	1	3	1		1	
feature5\.	L	M	L		L			1	3			1
feature5\subfeature1	H	M	M		M		1	3		1		
feature5\subfeature2	H	M	L		L		1	1	2		1	
feature5\subfeature3	L	M	L		L			1	3			1
feature6	H	H	H	M	M	M	3	3		1		
sharedlib	L	L	L	L	L	L			6			1
sharedlib\uicomponents	H	H	H	H	M	H	5	1		1		
other		L							1			1
JSP	M	L	L	L	L	L		1	5			1
application	M	L	L		L			1	3			1
tags		L	L		L				3			1
other			L		M			1	1		1	
CSS	M	L	L	M	L	L		2	4			1
										8	14	14

Effectiveness and Efficiency of RBT



MORE **TEST** **LESS**

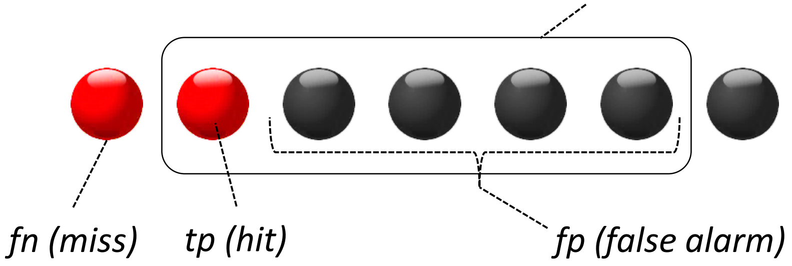
Effectiveness

- Finding more defects
- Finding defects earlier
- Finding the critical defects
- ...

Efficiency

- Reduce time of testing
- Reduce cost of testing
- ...

Selection: effectiveness,recall = 1/2 = 50%; efficiency,precision = 1/5 = 20%



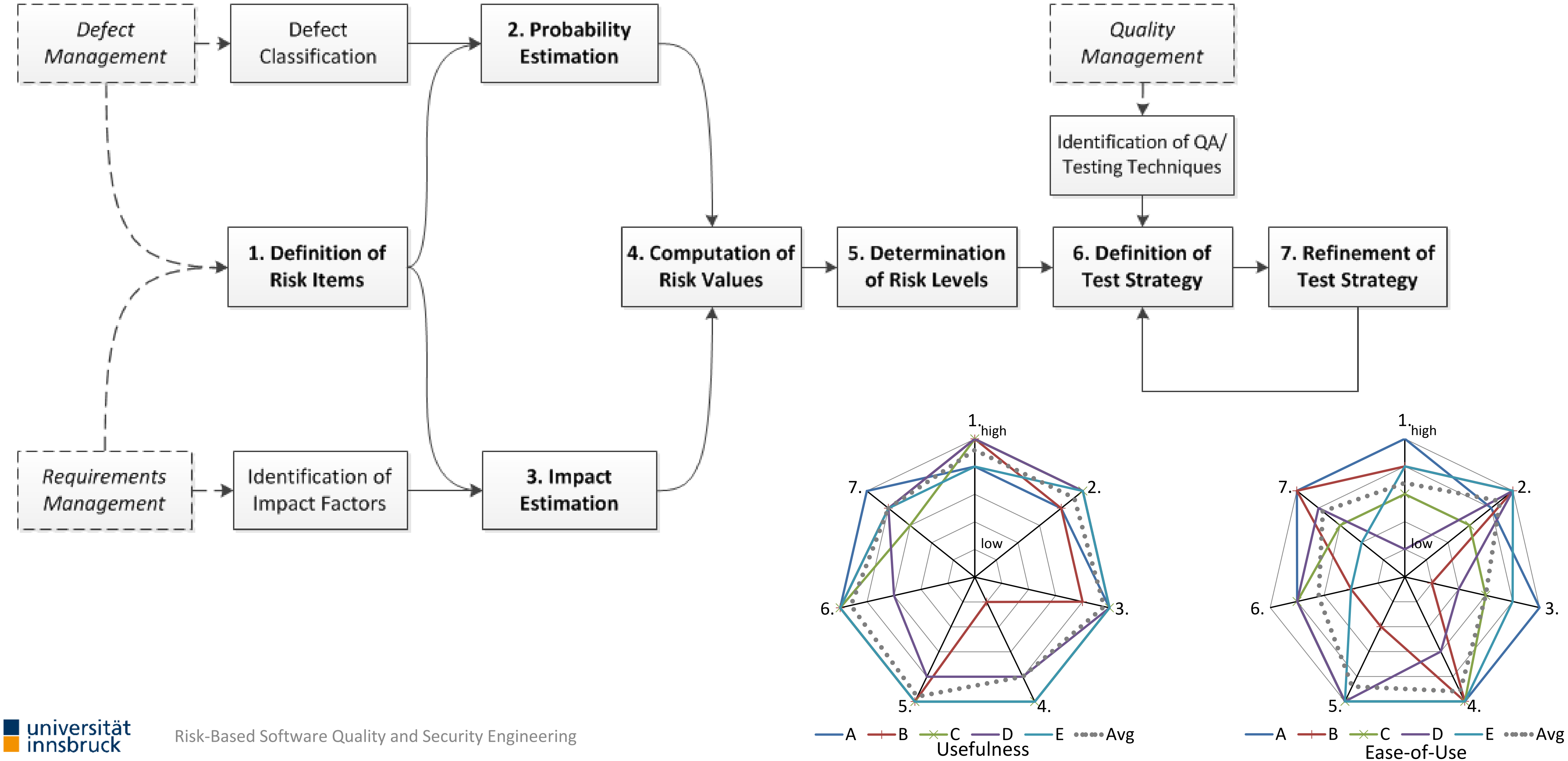
Risk-Based Testing in SME and Large Enterprises

Felderer, M., Ramler, R.: *Risk orientation in software testing processes of small and medium enterprises*. Software Quality Journal, 24(3), 519-548, 2016

Findings from SME	Rel.	Findings from large enterprises
Risk is an **implicit concept** and relies on subjective perception	<	Degree of **formality of risk** depends on the application scope, formality increases with wider scope and abstraction level
Risk is considered in **all testing activities**, even when not following an explicit risk-based testing approach	=	Risk is considered in **all testing activities**, even when not following an explicit risk-based testing approach
The understanding of risks is used to **adjust the amount of testing**, the overall test effort, or the established test budgets.	#	Risk-based testing is **not used to reduce the amount of testing**, the overall test effort, or the established test budgets
Make testing **more efficient**: selection of tests based on risks lead to a reduction of cost and time for testing	<	Make testing **more effective**: prioritization for detecting most critical defects first, reduces overall stabilization costs and time
Risk is used as rationale and **motivation** for the application of QA measures	<	Risk information used for **informed decision-making** and new insights to triangulate and refine decisions

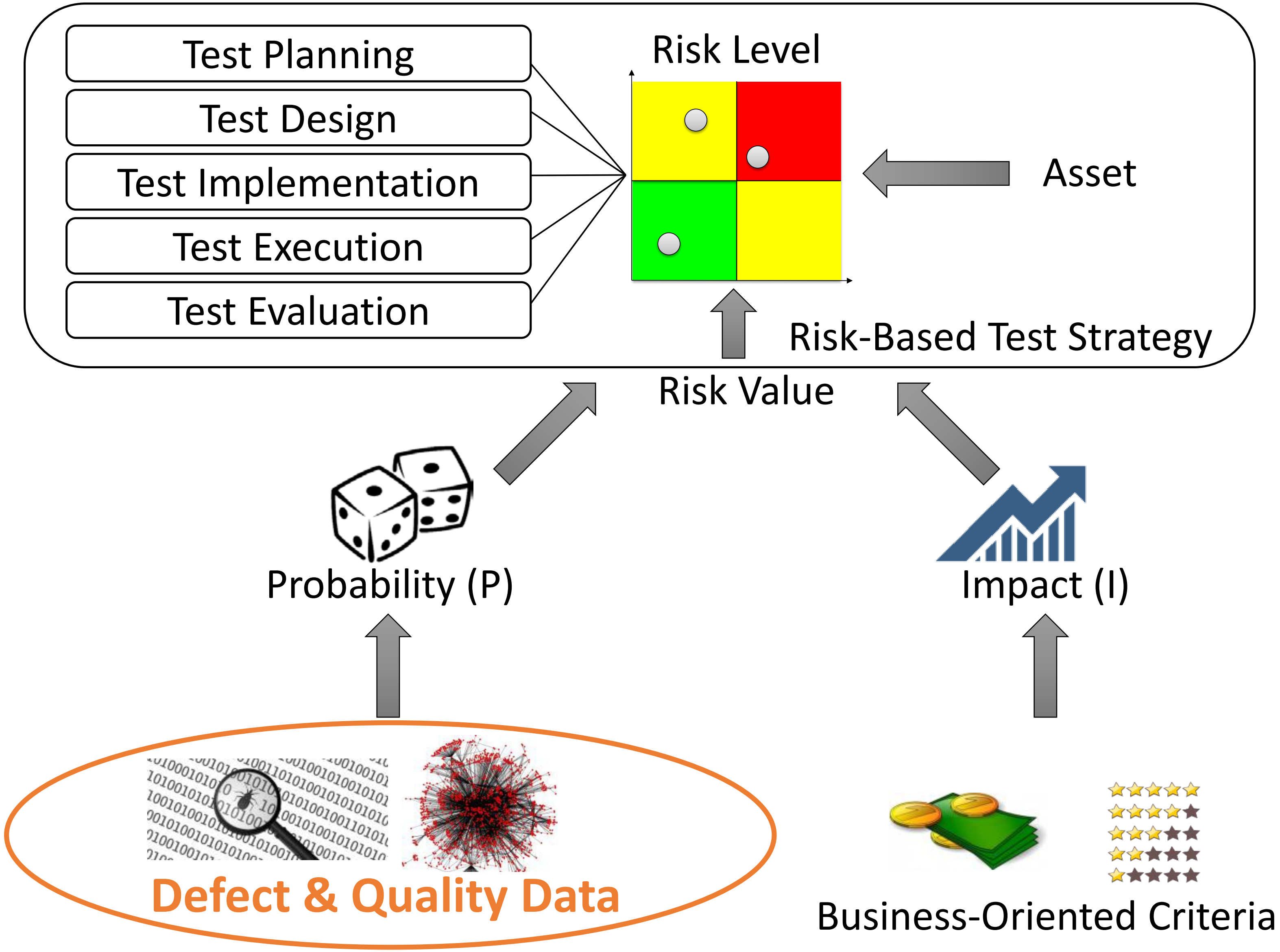
Risk-Based Test Strategy Development for SME

Ramler, R., Felderer, M.: *A Process for risk-based test strategy development and its industrial evaluation*. PROFES 2015, 355-371, 2015



Defect Management
Defect Classification
2. Probability Estimation
Quality Management
Identification of QA/ Testing Techniques
1. Definition of Risk Items
4. Computation of Risk Values
5. Determination of Risk Levels
6. Definition of Test Strategy
7. Refinement of Test Strategy
Requirements Management
Identification of Impact Factors
3. Impact Estimation
1.
high
low
2.
3.
4.
5.
6.
7.
A
B
C
D
E
Avg
Usefulness
1.
high
low
2.
3.
4.
5.
6.
7.
A
B
C
D
E
Avg
Ease-of-Use

Defect & Quality Data in Risk-Based Testing



Test Planning

Test Design

Test Implementation

Test Execution

Test Evaluation

Risk Level

Asset

Risk-Based Test Strategy

Risk Value

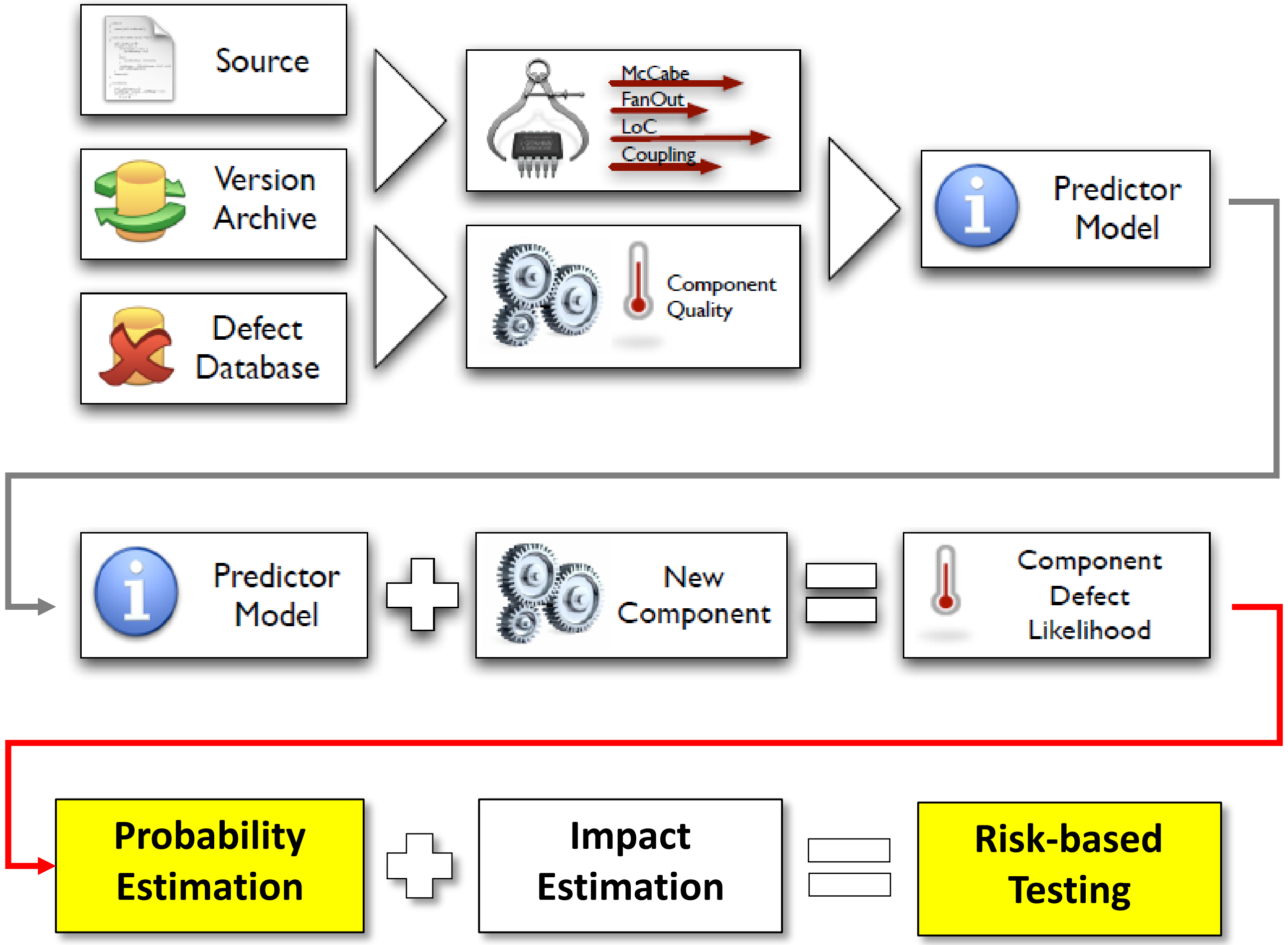
Probability (P)

Impact (I)

Defect & Quality Data

Business-Oriented Criteria

Data-Driven Probability Prediction



Probablity Prediction based on Defect History

Ramler, R., Felderer, M.: *A lightweight approach for estimating probability in risk-based software testing*. RISK 2016, 115-128, 2016

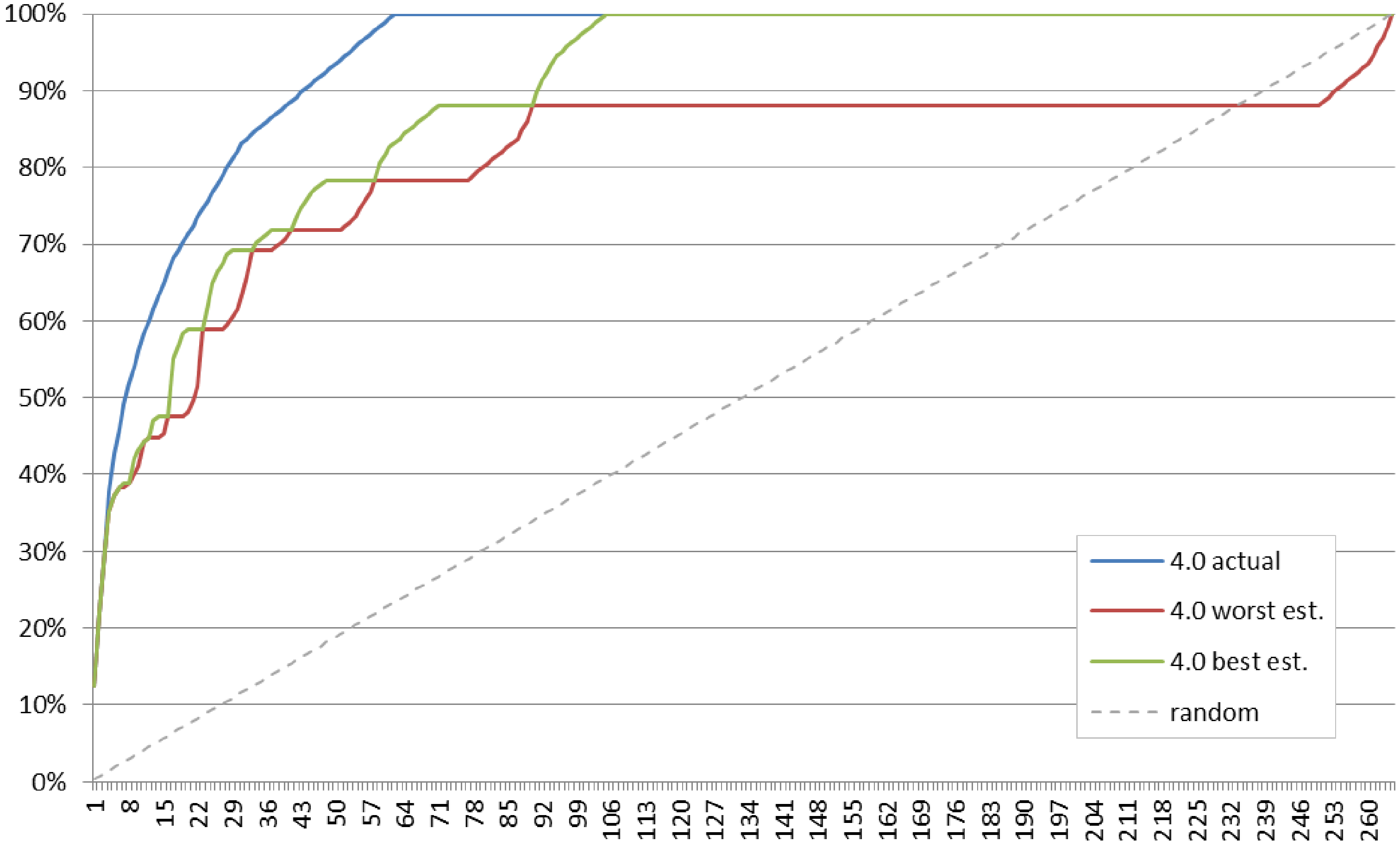
Yesterday‘s Weather Principle

Release	n	
	Defects	Probability
Component A	10	high
Component B	9	high
Component C	4	medium
Component D	1	low
Component E	0	low
Component F	0	low

n+1
Estimated Probability
high
high
medium
low
low
low

Evaluation of Yesterday‘s Weather Principle

Gain Chart and Confusion Matrix for JEdit 4.0 (based on data from v3.2)

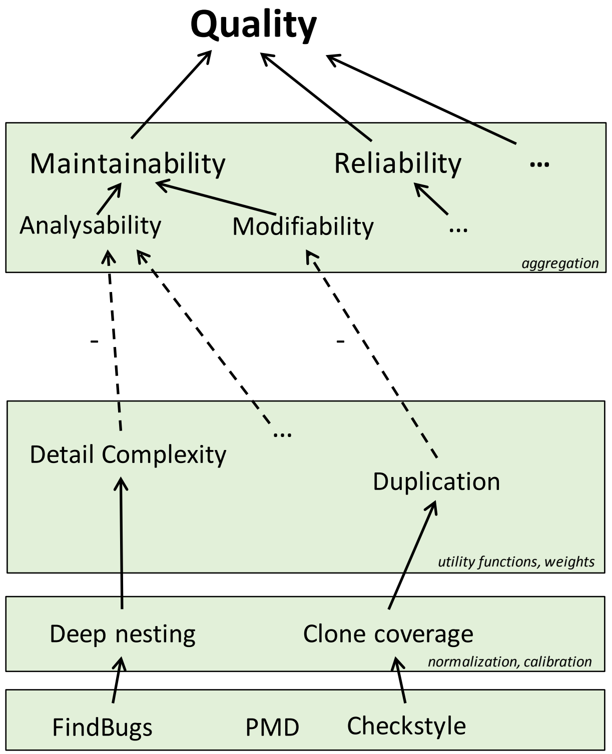


		estimated			
		high	medium	low	
actual	high	4%	0%	0%	4%
	medium	5%	9%	6%	19%
	low	4%	12%	60%	77%
		12%	22%	66%	100%

		estimated			
		high	medium	low	
actual	high	10	1	0	11
	medium	13	23	15	51
	low	10	33	160	203
		33	57	175	265

Probability Estimation based on Quality Metrics

Foidl, H., Felderer, M.: *Integrating software quality models into risk-based testing*. Software Quality Journal, 26(2), 809-847, 2018



Quality

Maintainability, Reliability, …

Analysability, Modifiability, …

aggregation

-

-

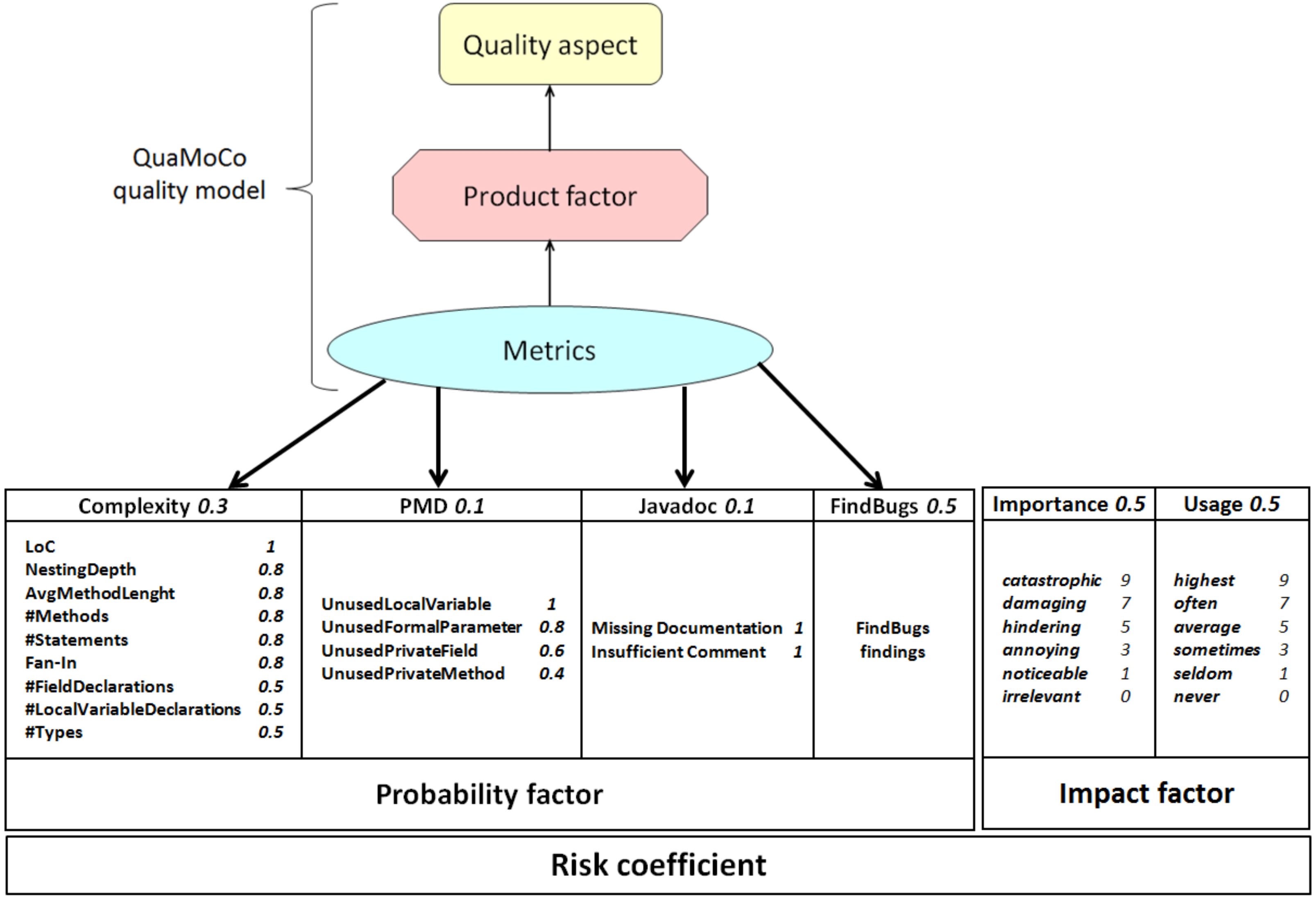
Detail Complexity, …, Duplication

utility functions, weights

Deep nesting, Clone coverage

normalization, calibration

FindBugs, PMD, Checkstyle



QuaMoCo quality model

Quality aspect

Product factor

Metrics

Complexity *0.3*		PMD *0.1*		Javadoc *0.1*		FindBugs *0.5*
LoC	*1*	UnusedLocalVariable	*1*	Missing Documentation	*1*	FindBugs findings
NestingDepth	*0.8*	UnusedFormalParameter	*0.8*	Insufficient Comment	*1*	
AvgMethodLenght	*0.8*	UnusedPrivateField	*0.6*			
#Methods	*0.8*	UnusedPrivateMethod	*0.4*			
#Statements	*0.8*					
Fan-In	*0.8*					
#FieldDeclarations	*0.5*					
#LocalVariableDeclarations	*0.5*					
#Types	*0.5*					

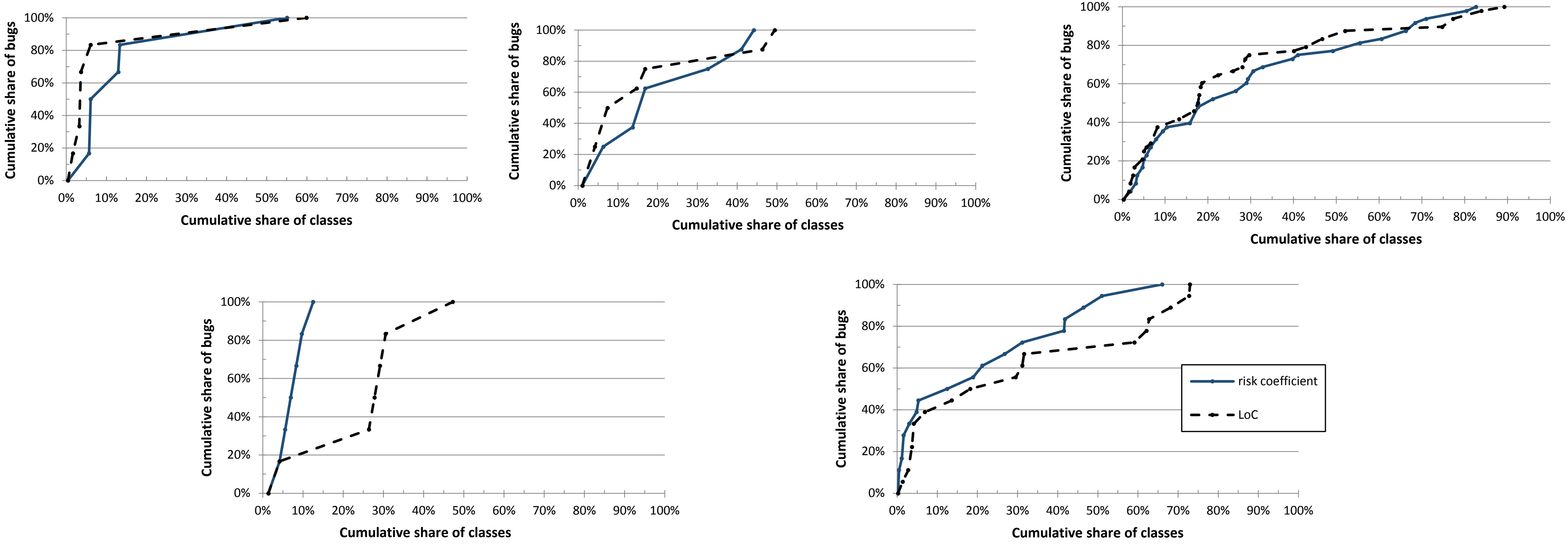
Probability factor

Importance *0.5*		Usage *0.5*	
catastrophic	*9*	*highest*	*9*
damaging	*7*	*often*	*7*
hindering	*5*	*average*	*5*
annoying	*3*	*sometimes*	*3*
noticeable	*1*	*seldom*	*1*
irrelevant	*0*	*never*	*0*

Impact factor

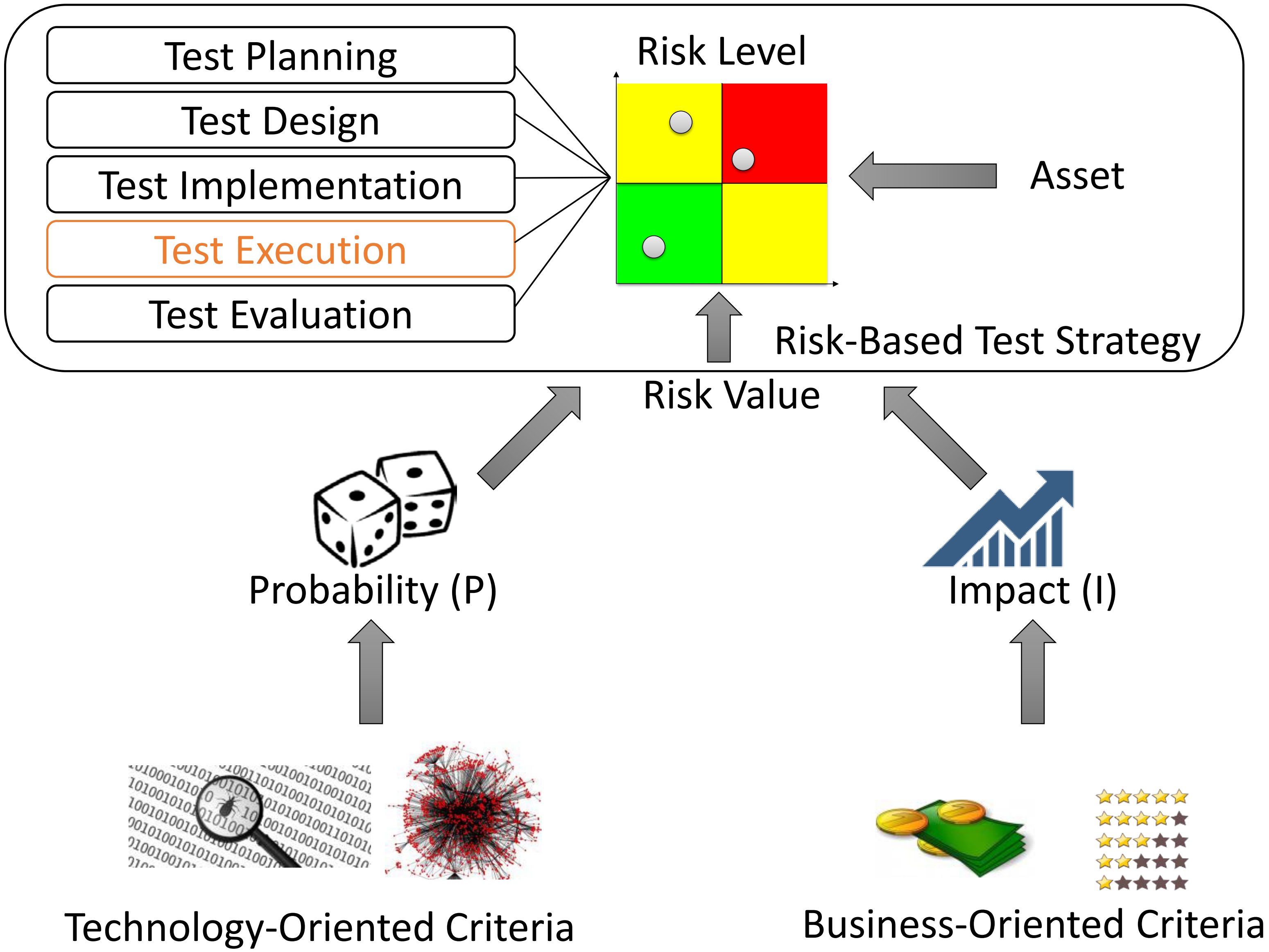
Risk coefficient

Evaluation of Metrics-Based Estimation



Software product	Versions	LoC	RBT
Apache Commons IO	1.4-2.1	47%	10%
Apache PDFBox	1.0.0-1.8.9	73%	66%
Google Guava	10.0-18.0	89%	83%
JUnit	4.6-4.12	60%	55%
Mockito	1.0- 1.10.19	50%	44%
Total average		63.8%	51.6%

Risk-Based Test Strategy



Test Planning

Test Design

Test Implementation

Test Execution

Test Evaluation

Risk Level

Asset

Risk-Based Test Strategy

Risk Value

Probability (P)

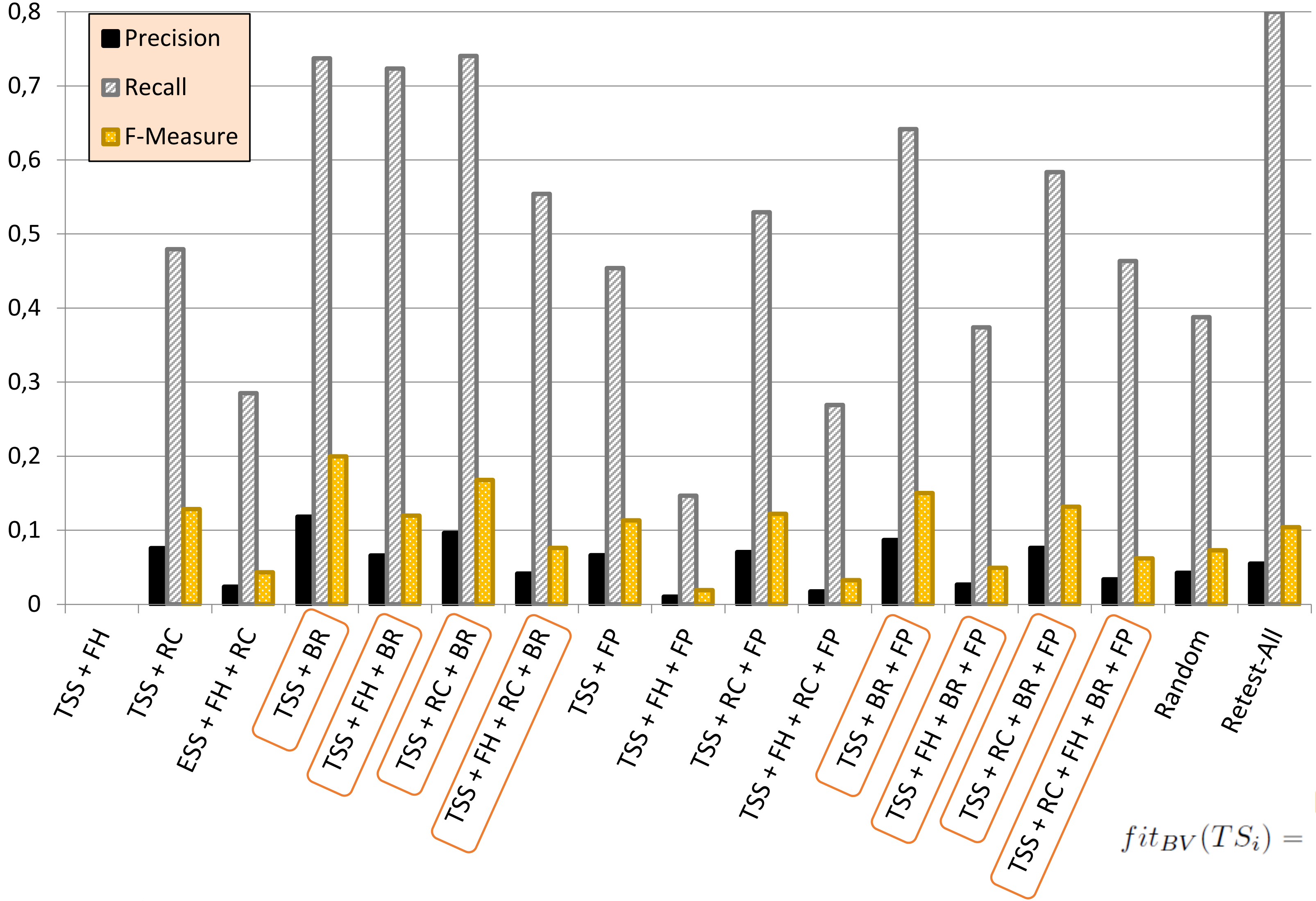
Impact (I)

Technology-Oriented Criteria

Business-Oriented Criteria

Risk-Based System Test Case Selection

Lachmann R., Felderer, M. et al.: *Multi-objective black box test case selection for system testing*. GECCO 2017, 1311-1318, 2017

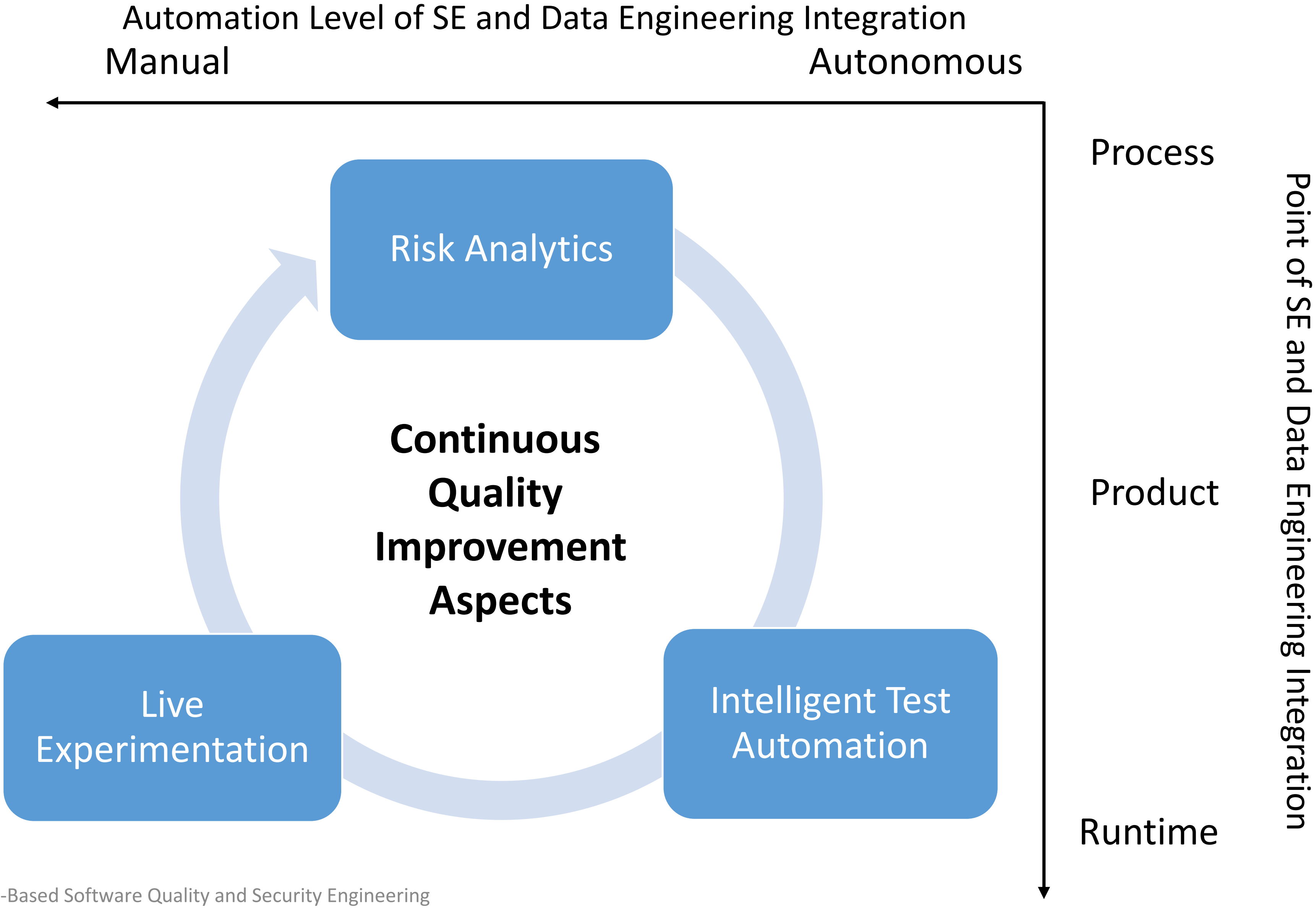


Min:
TSS: Test Set Size

Max:
RC: Req Coverage
FH: Failure History
BR: Business Relevance
FP: Failure Probability
EC: Execution Cost
LE: Last Execution

$$fit_{BV}(TS_i) = \sum_{j=0}^{|TS_i|} \sum_{k=0}^{|Req(tc_j)|} busval(req_k), req_k \in Req(tc_j)$$

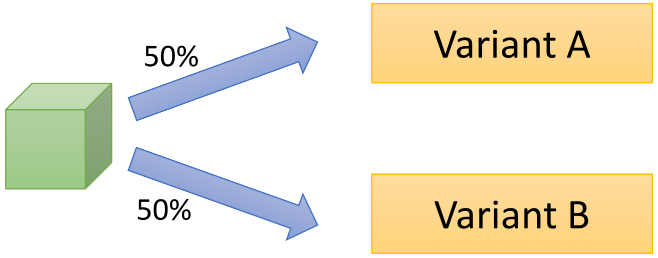
Vision for Risk-Based Quality Assurance



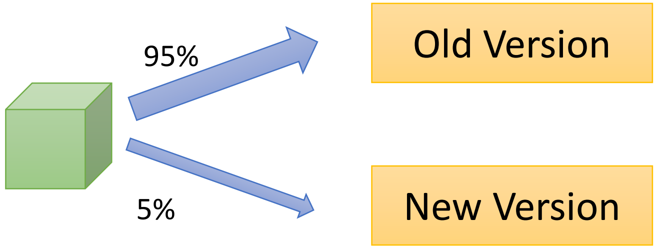
Automation Level of SE and Data Engineering Integration
Manual
Autonomous
Process
Product
Runtime
Point of SE and Data Engineering Integration
Risk Analytics
Continuous Quality Improvement Aspects
Intelligent Test Automation
Live Experimentation

External and Internal Experimentation Approaches

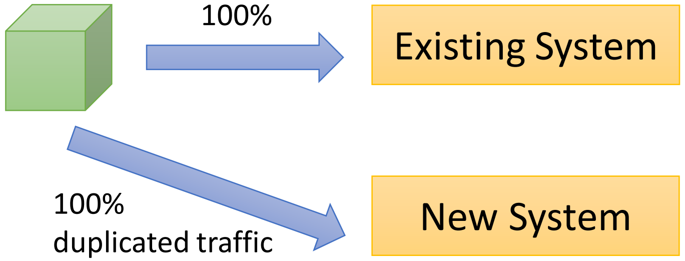
A/B Test

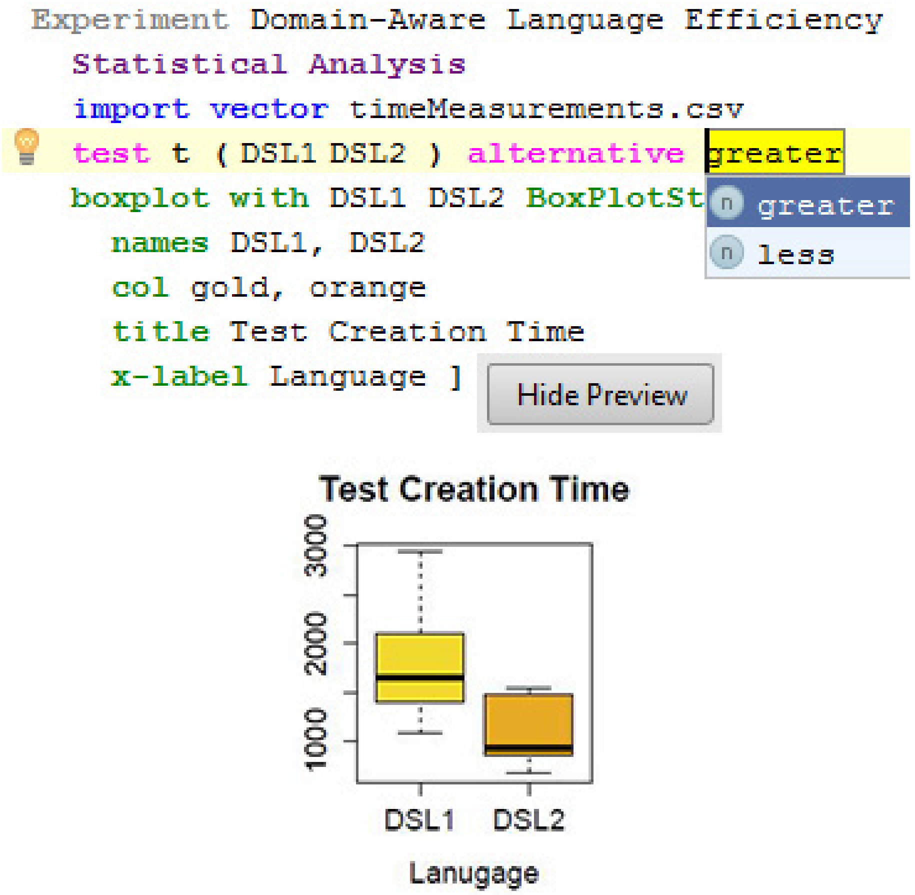


Canary Release



Dark Launch

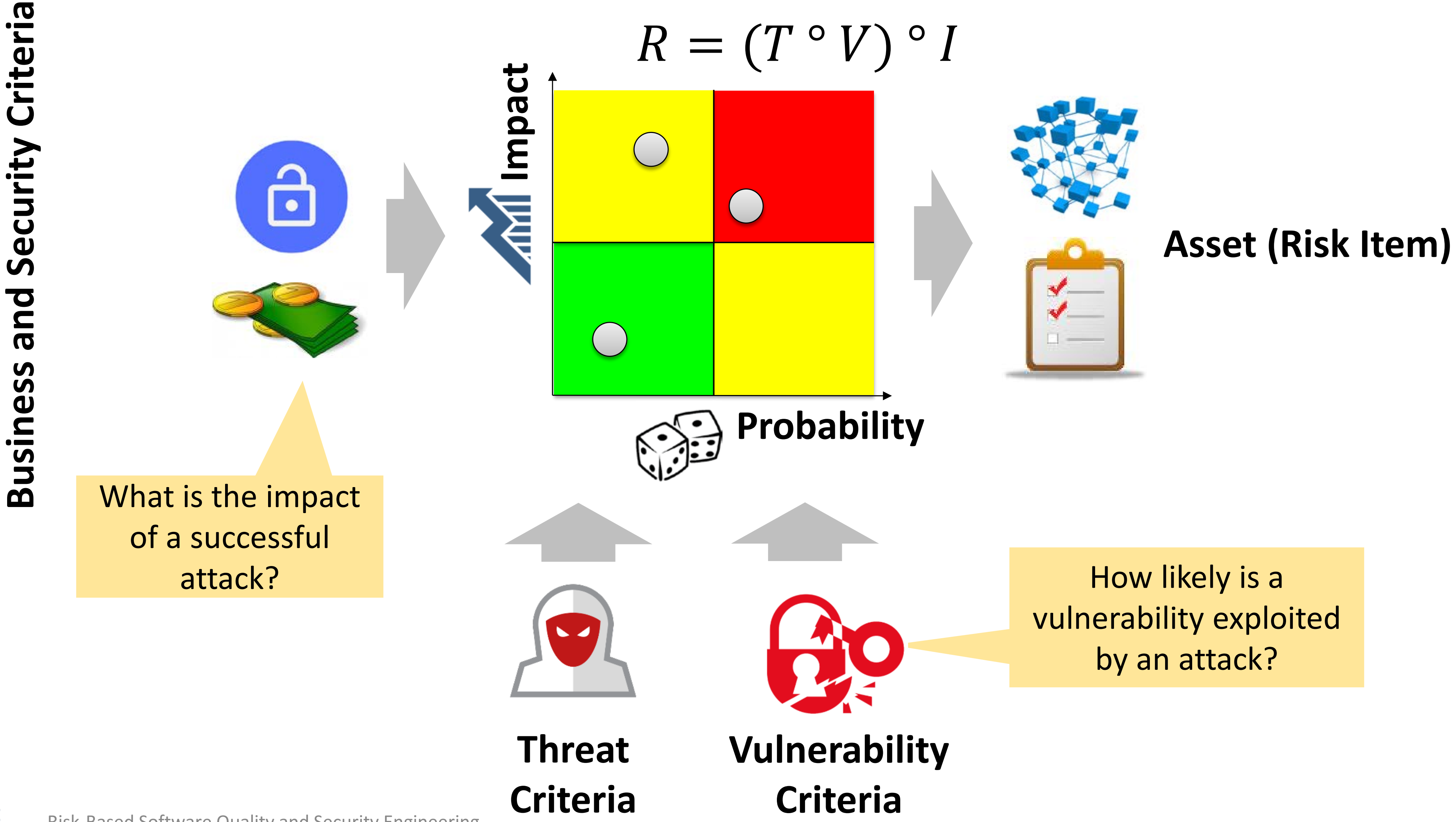




```
Experiment Domain-Aware Language Efficiency
  Statistical Analysis
  import vector timeMeasurements.csv
  test t ( DSL1 DSL2 ) alternative greater
  boxplot with DSL1 DSL2 BoxPlotSt
    names DSL1, DSL2
    col gold, orange
    title Test Creation Time
    x-label Language ]
```

Risk Concept in Software Security Engineering

$$R = (T \circ V) \circ I$$



Business and Security Criteria

Impact

Probability

Asset (Risk Item)

What is the impact of a successful attack?

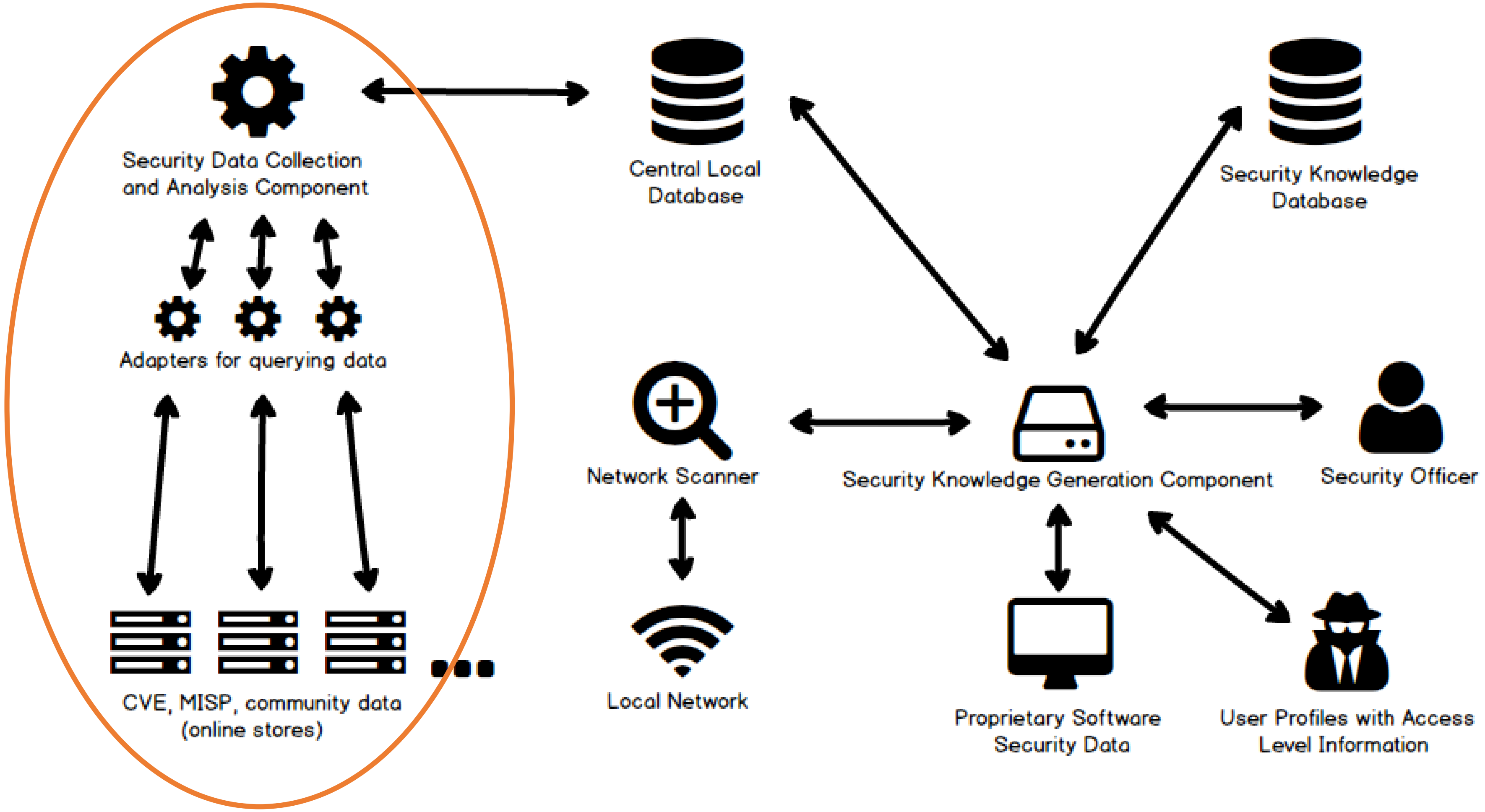
How likely is a vulnerability exploited by an attack?

Threat Criteria

Vulnerability Criteria

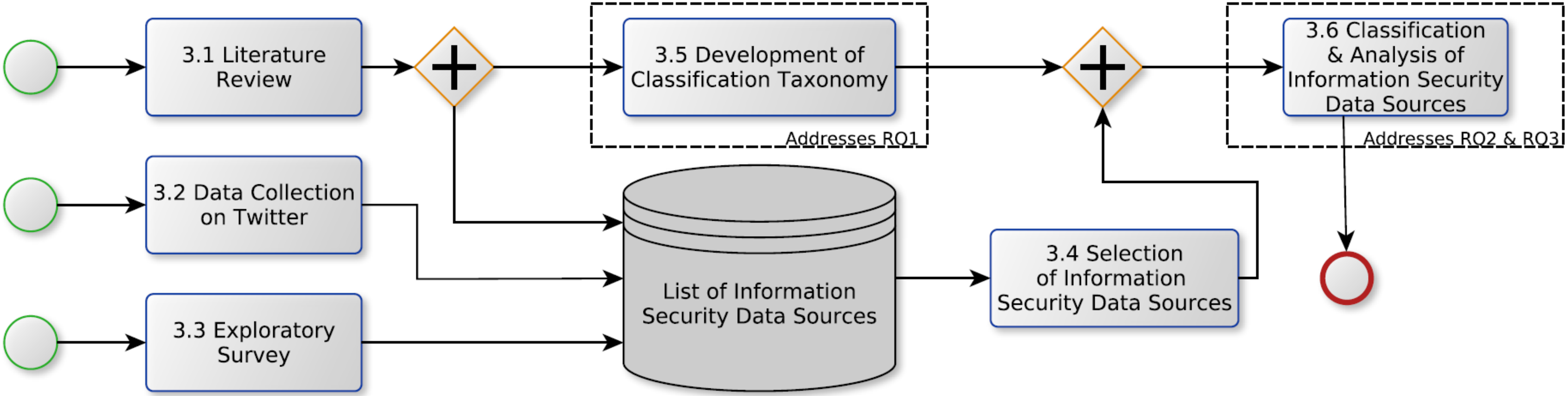
Security Knowledge Extraction and Application

Felderer, M., Pekaric, I.: *Research Challenges in Empowering Agile Teams with Security Knowledge Based on Public and Private Information Sources*. SecSE@ESORICS 2017, 1-7, 2017

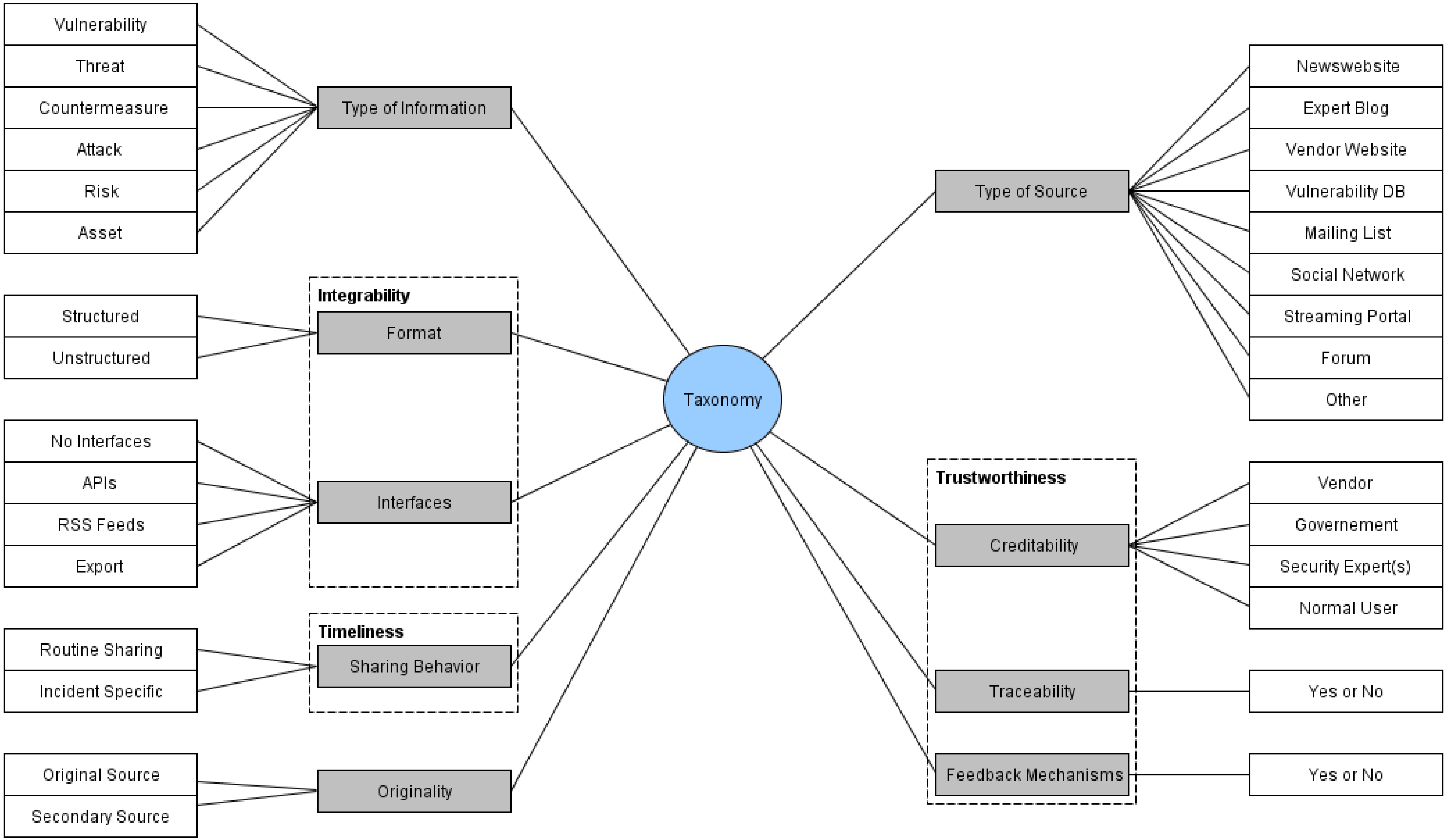

Security Data Collection and Analysis Component
Adapters for querying data
CVE, MISP, community data (online stores)
Central Local Database
Security Knowledge Database
Network Scanner
Local Network
Security Knowledge Generation Component
Security Officer
Proprietary Software Security Data
User Profiles with Access Level Information

Analysis of Public Security Risk Data Sources: Method

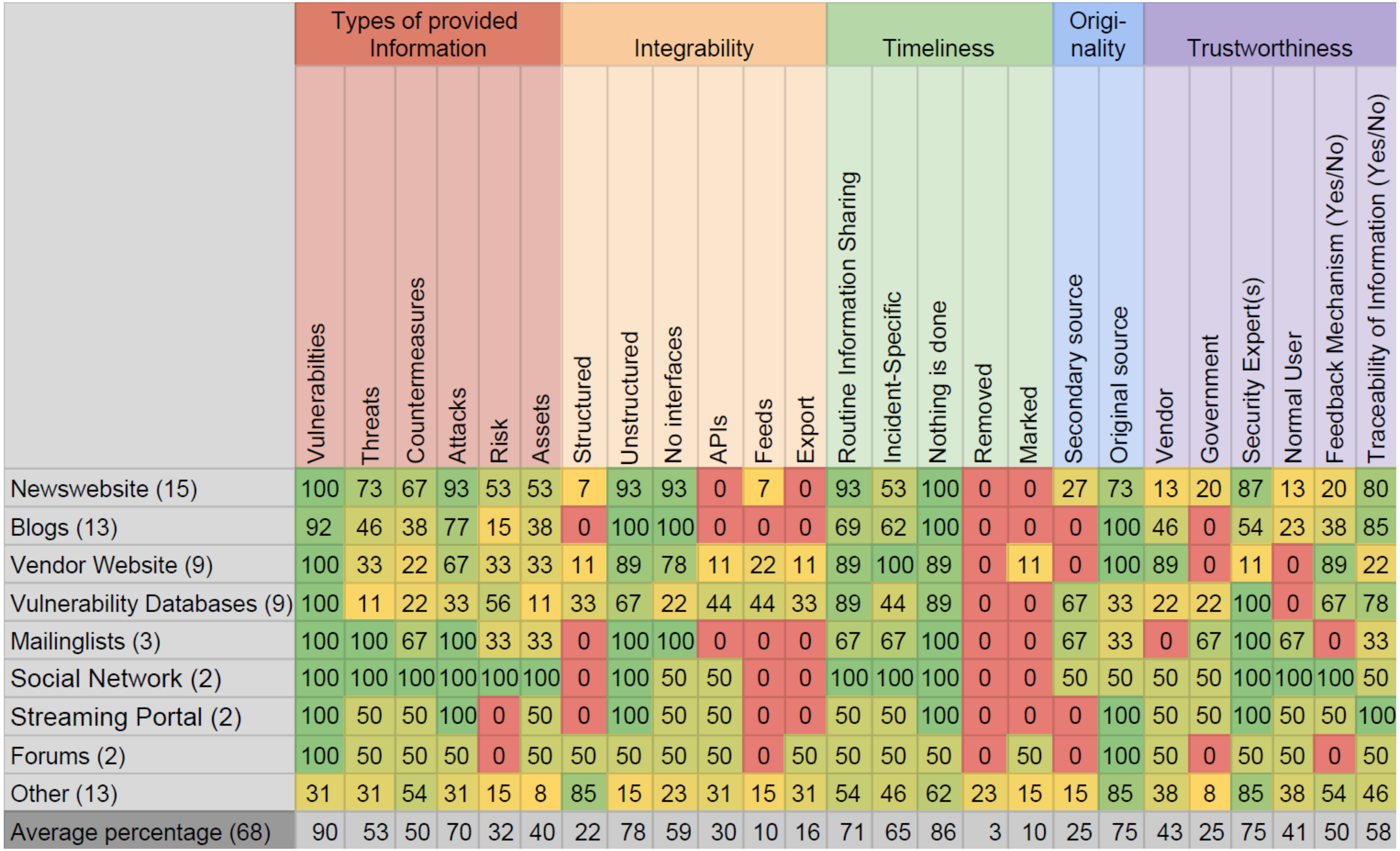
Sauerwein, C., Pekaric, I., Felderer, M., Breu R.: *An Analysis and Classification of Public Information Security Data Sources used in Research and Practice*. Computers & Security, 2018


3.1 Literature Review
3.2 Data Collection on Twitter
3.3 Exploratory Survey
3.5 Development of Classification Taxonomy
Addresses RQ1
List of Information Security Data Sources
3.4 Selection of Information Security Data Sources
3.6 Classification & Analysis of Information Security Data Sources
Addresses RQ2 & RQ3

Taxonomy of Security Risk Data Sources

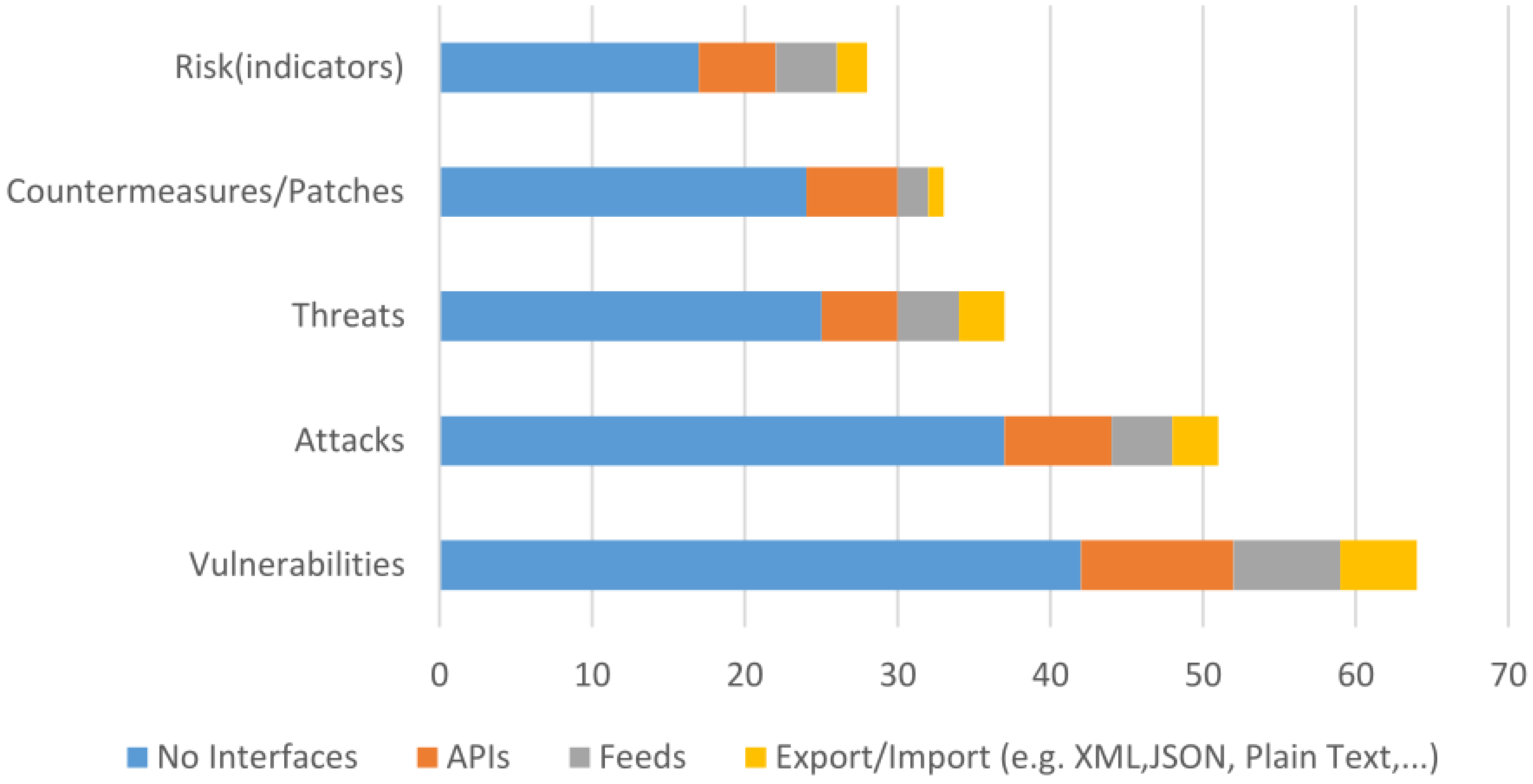


Classification of Security Risk Data Sources

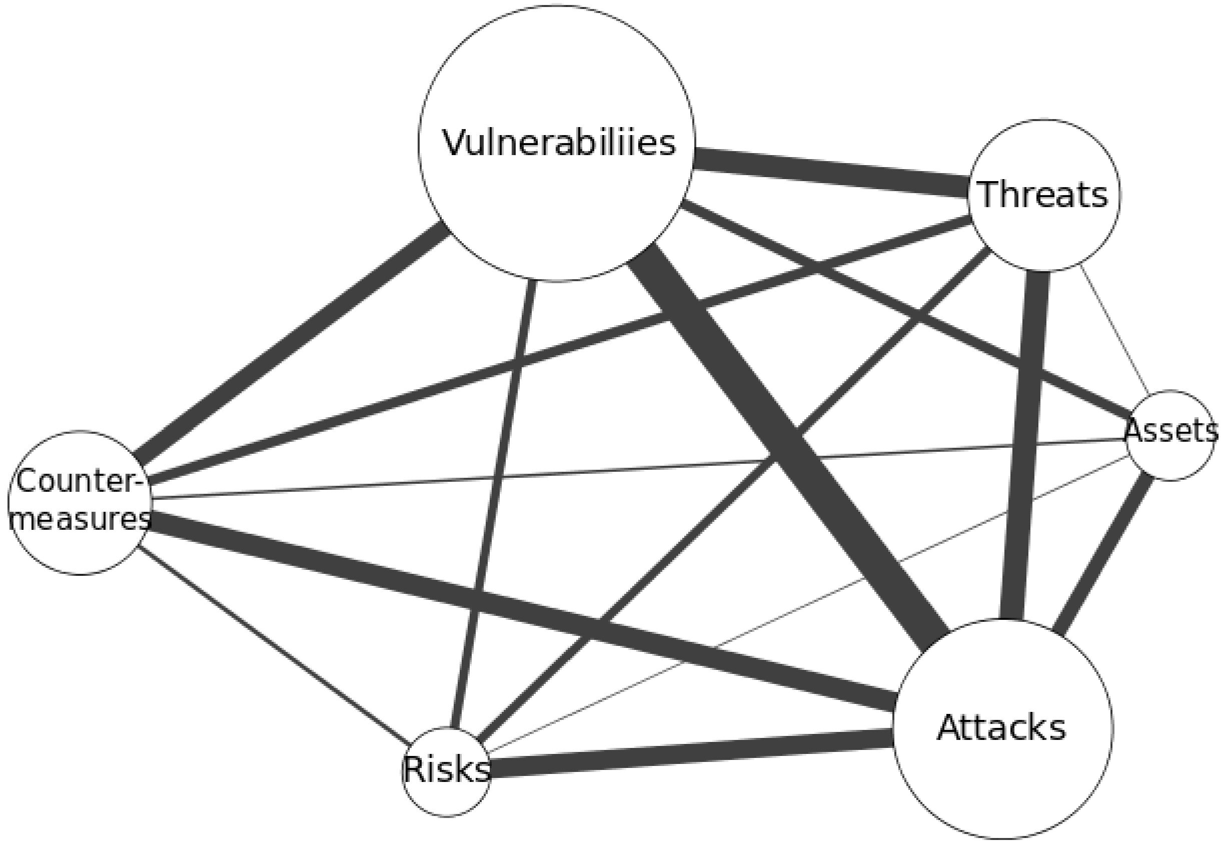


	Types of provided Information						Integrability						Timeliness					Originality		Trustworthiness					
	Vulnerabilties	Threats	Countermeasures	Attacks	Risk	Assets	Structured	Unstructured	No interfaces	APIs	Feeds	Export	Routine Information Sharing	Incident-Specific	Nothing is done	Removed	Marked	Secondary source	Original source	Vendor	Government	Security Expert(s)	Normal User	Feedback Mechanism (Yes/No)	Traceability of Information (Yes/No)
Newswebsite (15)	100	73	67	93	53	53	7	93	93	0	7	0	93	53	100	0	0	27	73	13	20	87	13	20	80
Blogs (13)	92	46	38	77	15	38	0	100	100	0	0	0	69	62	100	0	0	0	100	46	0	54	23	38	85
Vendor Website (9)	100	33	22	67	33	33	11	89	78	11	22	11	89	100	89	0	11	0	100	89	0	11	0	89	22
Vulnerability Databases (9)	100	11	22	33	56	11	33	67	22	44	44	33	89	44	89	0	0	67	33	22	22	100	0	67	78
Mailinglists (3)	100	100	67	100	33	33	0	100	100	0	0	0	67	67	100	0	0	67	33	0	67	100	67	0	33
Social Network (2)	100	100	100	100	100	100	0	100	50	50	0	0	100	100	100	0	0	50	50	50	50	100	100	100	50
Streaming Portal (2)	100	50	50	100	0	50	0	100	50	50	0	0	50	50	100	0	0	0	100	50	50	100	50	50	100
Forums (2)	100	50	50	50	0	50	50	50	50	50	0	50	50	50	50	0	50	0	100	50	0	50	50	0	50
Other (13)	31	31	54	31	15	8	85	15	23	31	15	31	54	46	62	23	15	15	85	38	8	85	38	54	46
Average percentage (68)	90	53	50	70	32	40	22	78	59	30	10	16	71	65	86	3	10	25	75	43	25	75	41	50	58

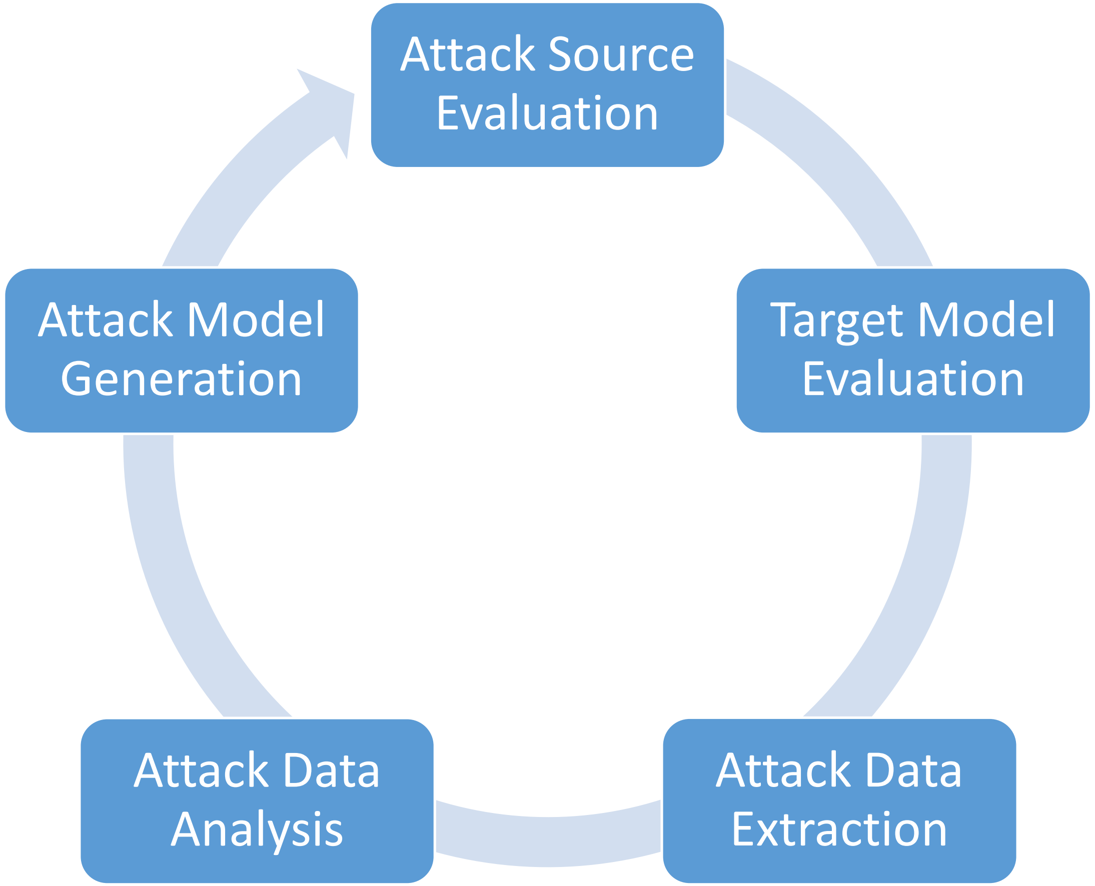
Interfaces Per Security Risk Data Source Type



Co-Occurence of Security Risk Data Source Types



Attack Model Mining



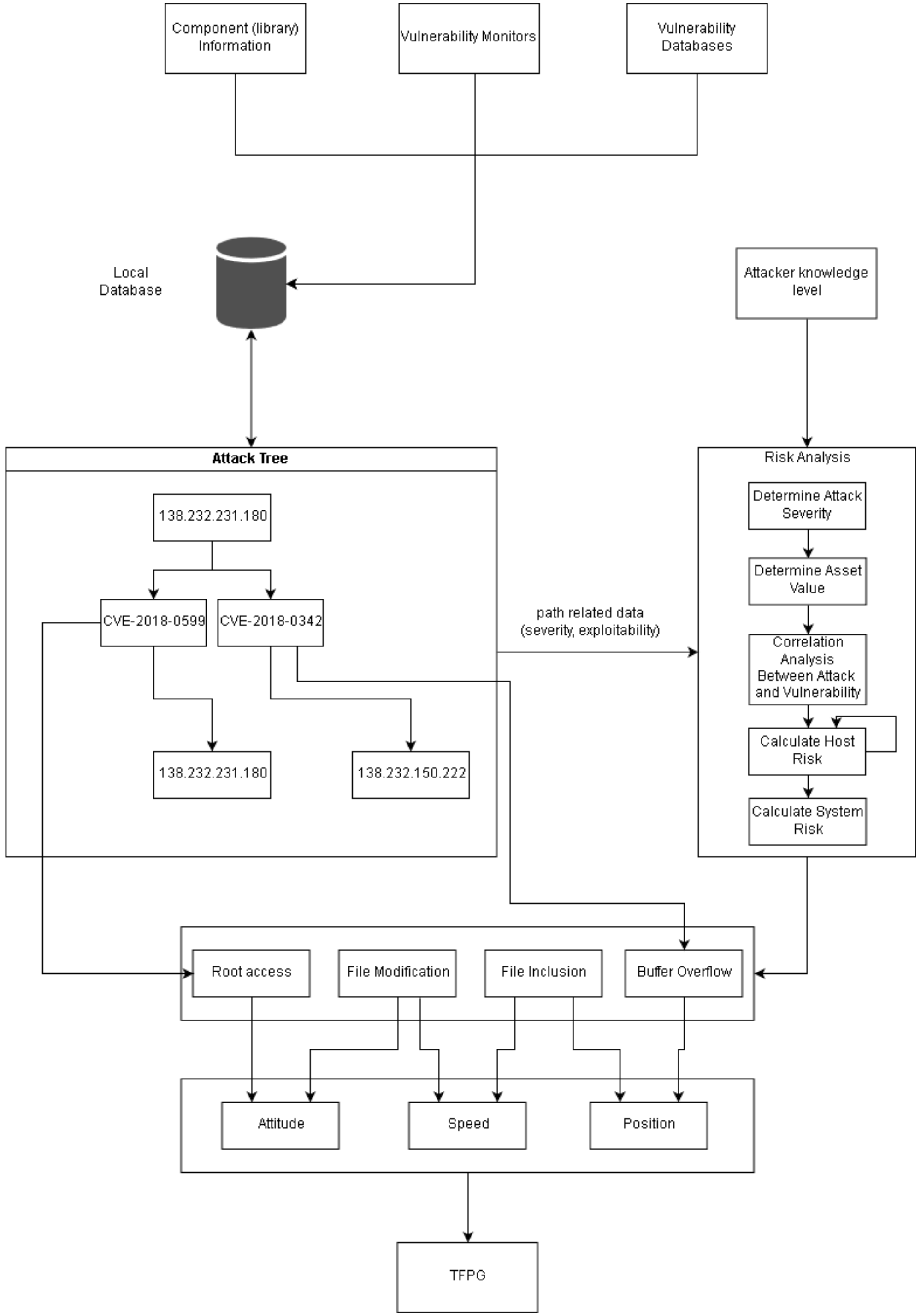
Attack Source Evaluation

Target Model Evaluation

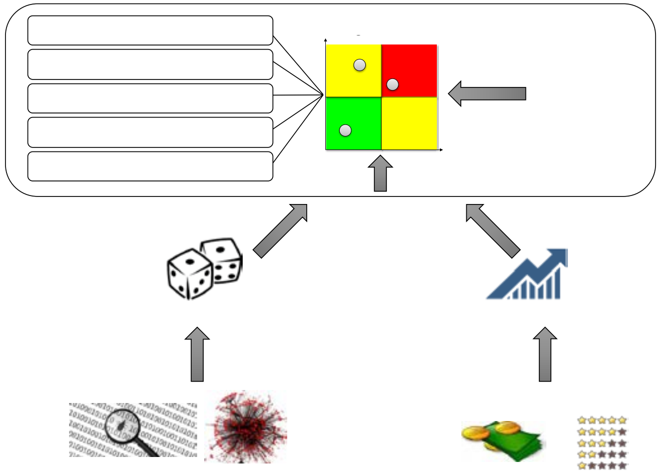
Attack Data Extraction

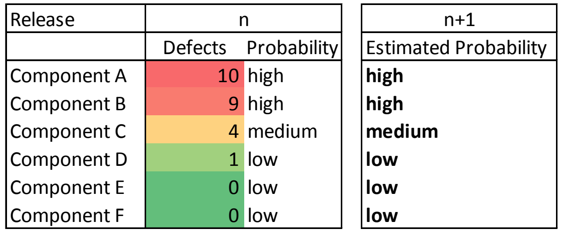
Attack Data Analysis

Attack Model Generation

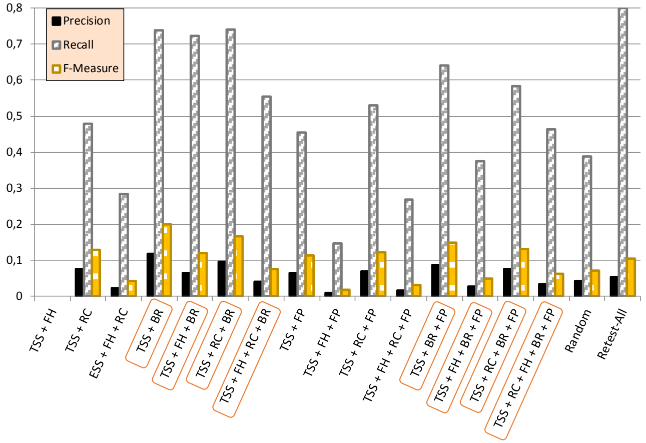


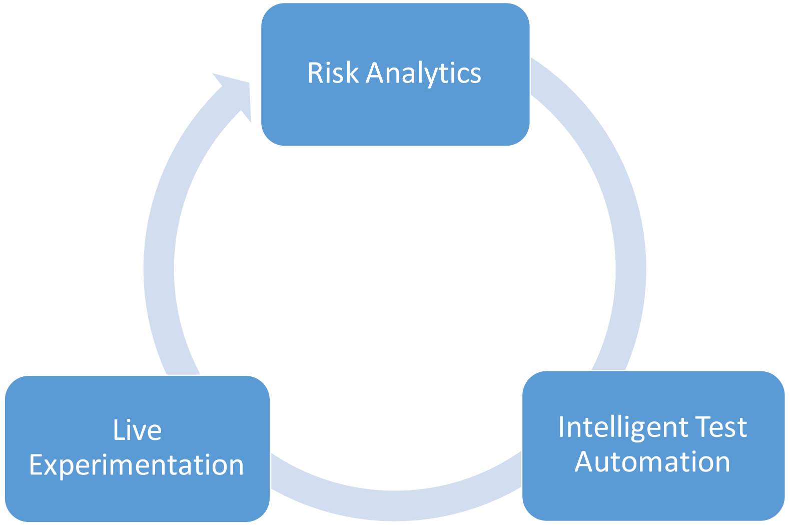
Summary

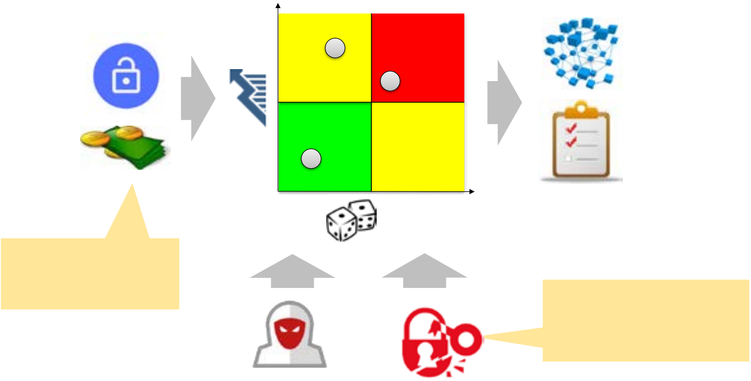


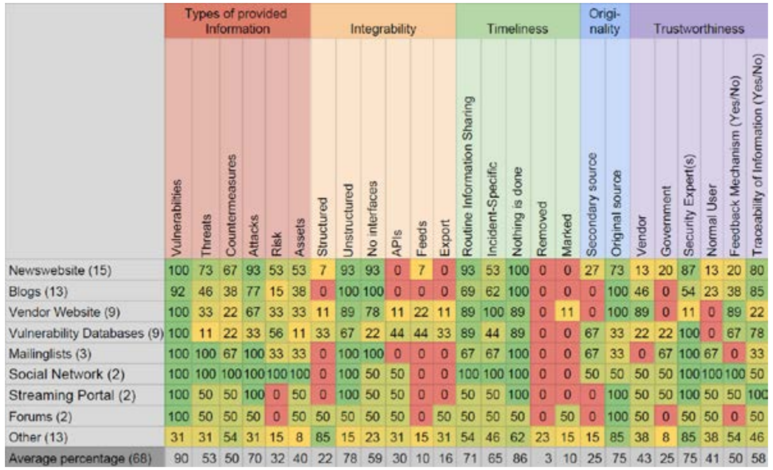


Release	n		n+1
	Defects	Probability	Estimated Probability
Component A	10	high	**high**
Component B	9	high	**high**
Component C	4	medium	**medium**
Component D	1	low	**low**
Component E	0	low	**low**
Component F	0	low	**low**

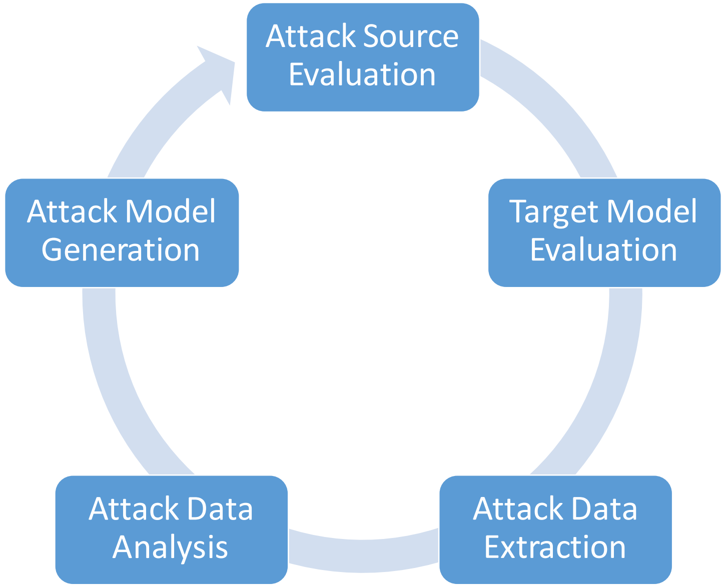








	Types of provided Information						Integrability						Timeliness					Originality		Trustworthiness					
	Vulnerabilities	Threats	Countermeasures	Attacks	Risk	Assets	Structured	Unstructured	No interfaces	APIs	Feeds	Export	Routine Information Sharing	Incident-Specific	Nothing is done	Removed	Marked	Secondary source	Original source	Vendor	Government	Security Expert(s)	Normal User	Feedback Mechanism (Yes/No)	Traceability of Information (Yes/No)
Newswebsite (15)	100	73	67	93	53	53	7	93	93	0	7	0	93	53	100	0	0	27	73	13	20	87	13	20	80
Blogs (13)	92	46	38	77	15	38	0	100	100	0	0	0	69	62	100	0	0	0	100	46	0	54	23	38	85
Vendor Website (9)	100	33	22	67	33	33	11	89	78	11	22	11	89	100	89	0	11	0	100	89	0	11	0	89	22
Vulnerability Databases (9)	100	11	22	33	56	11	33	67	22	44	44	33	89	44	89	0	0	67	33	22	22	100	0	67	78
Mailinglists (3)	100	100	67	100	33	33	0	100	100	0	0	0	67	67	100	0	0	67	33	0	67	100	67	0	33
Social Network (2)	100	100	100	100	100	100	0	100	50	50	0	0	100	100	100	0	0	50	50	50	50	100	100	100	50
Streaming Portal (2)	100	50	50	100	0	50	0	100	50	50	0	0	50	50	100	0	0	0	100	50	50	100	50	50	100
Forums (2)	100	50	50	50	0	50	50	50	50	50	0	50	50	50	50	0	50	0	100	50	0	50	50	0	50
Other (13)	31	31	54	31	15	8	85	15	23	31	15	31	54	46	62	23	15	15	85	38	8	85	38	54	46
Average percentage (68)	90	53	50	70	32	40	22	78	59	30	10	16	71	65	86	3	10	25	75	43	25	75	41	50	58



References

[1] Felderer, M., Schieferdecker, I.: *A taxonomy of risk-based testing*. Software Tools for Technology Transfer, 16(5), 559-568, 2014

[2] Felderer, M., Ramler, R.: *Integrating risk-based testing in industrial test processes*. Software Quality Journal, 22(3), 543-575, 2014

[3] Felderer, M., Ramler, R.: *Risk orientation in software testing processes of small and medium enterprises*. Software Quality Journal, 24(3), 519-548, 2016

[4] Ramler, R., Felderer, M.: *A process for risk-based test strategy development and its industrial evaluation*. PROFES 2015, 355-371, 2015

[5] Ramler, R., Felderer, M.: *A lightweight approach for estimating probability in risk-based software testing*. RISK 2016, 115-128, 2016

[6] Foidl, H., Felderer, M.: *Integrating software quality models into risk-based testing*. Software Quality Journal, 26(2), 809-847, 2018

[7] Lachmann R., Felderer, M. et al.: *Multi-objective black box test case selection for system testing*. GECCO 2017, 1311-1318, 2017

[8] Felderer, M., Pekaric, I.: *Research Challenges in Empowering Agile Teams with Security Knowledge Based on Public and Private Information Sources*. SecSE@ESORICS 2017, 1-7, 2017

[9] Sauerwein, C., Pekaric, I., Felderer, M., Breu R.: *An Analysis and Classification of Public Information Security Data Sources used in Research and Practice*. Computers & Security, 2018 (under revision)

universität
innsbruck

Risk-Based Software Quality and Security Engineering in Data-Intensive Environments

Prof. Dr. Michael Felderer

Department of Computer Science

Universität Innsbruck

Austria

✉ michael.felderer@uibk.ac.at

@mfelderer