

Die Rolle der OSS Compliance Zertifizierung im Software-Beschaffungsprozess – Vorstellung einer wissenschaftlichen Studie

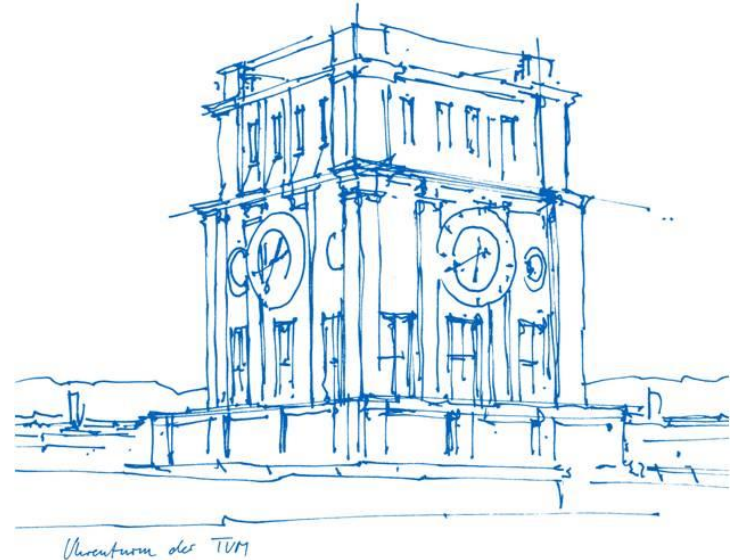
Juliane Wissel (Technische Universität München)

Michael Zaggl (Aarhus University)

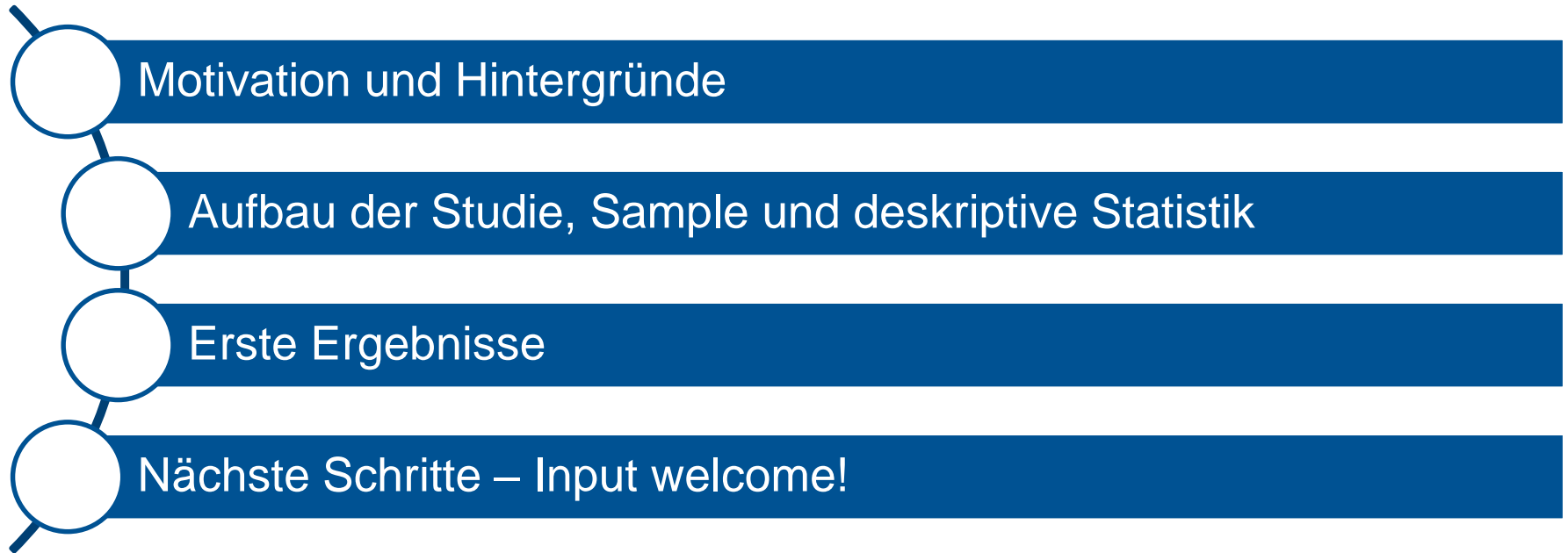
Jörn Block (Universität Trier)

29. September 2022

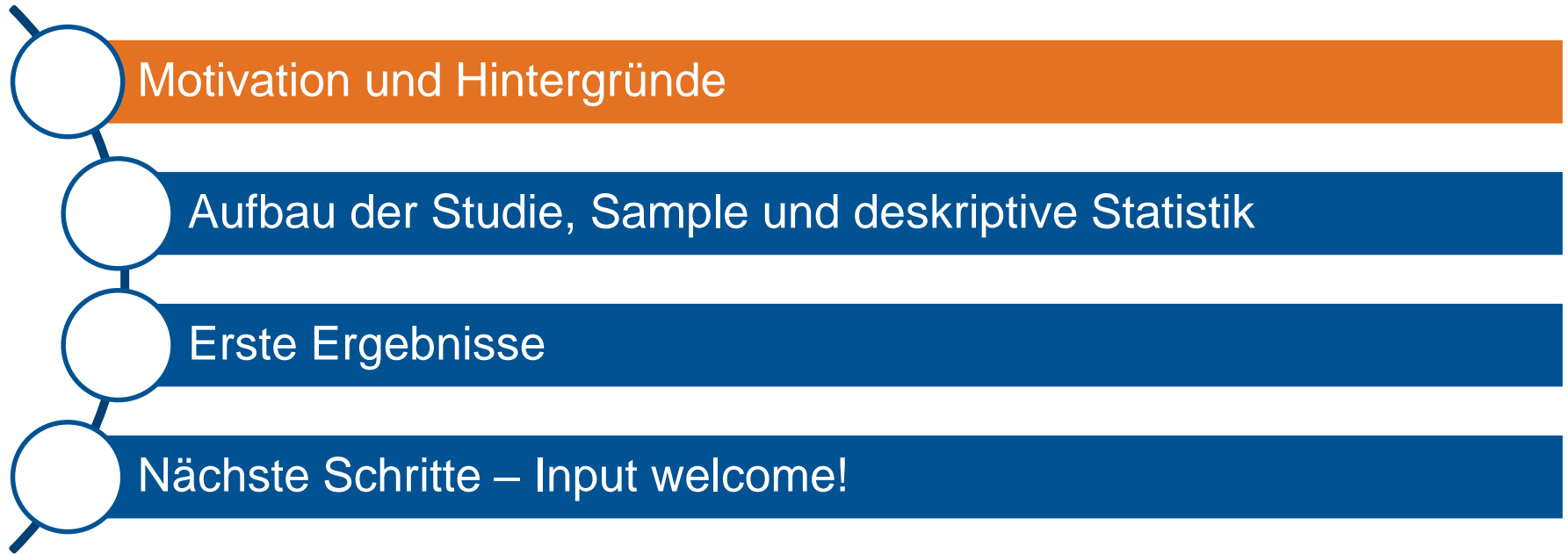
Bitkom Forum Open Source, Erfurt



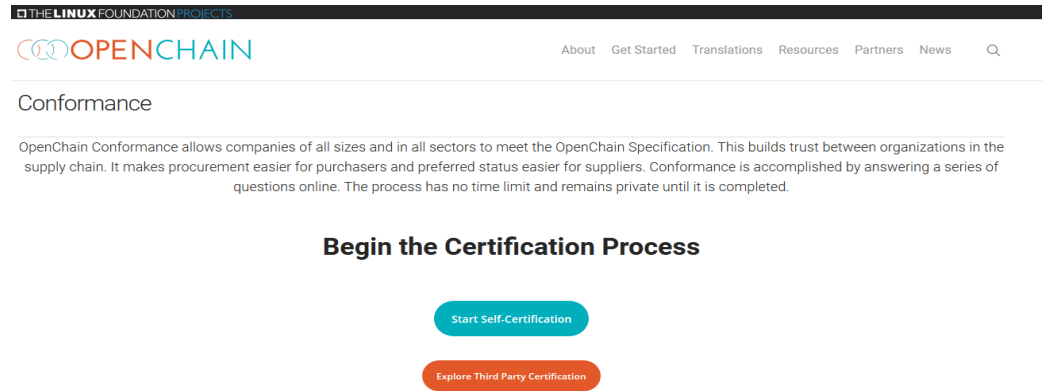
Agenda



Agenda



Das Phänomen: Zertifizierung von OSS Compliance Programmen



THE LINUX FOUNDATION PROJECTS

OPENCHAIN

About Get Started Translations Resources Partners News Q

Conformance

OpenChain Conformance allows companies of all sizes and in all sectors to meet the OpenChain Specification. This builds trust between organizations in the supply chain. It makes procurement easier for purchasers and preferred status easier for suppliers. Conformance is accomplished by answering a series of questions online. The process has no time limit and remains private until it is completed.

Begin the Certification Process

Start Self-Certification

Explore Third Party Certification

- OpenChain Spezifikation: Industriestandard für OSS Compliance im SW-Beschaffungsprozess
- Wesentliche Elemente: Dokumentierte Open Source Policy, klar definierte Rollen/Verantwortlichkeiten hinsichtlich OSS Compliance, Lizenz-Review-Prozess, Bereitstellung einer SBOM
- Seit Ende 2020: Offizieller ISO Standard (ISO 5230)
- Zertifizierung: Selbstzertifizierung vs. Zertifizierung durch Zertifizierungsstelle

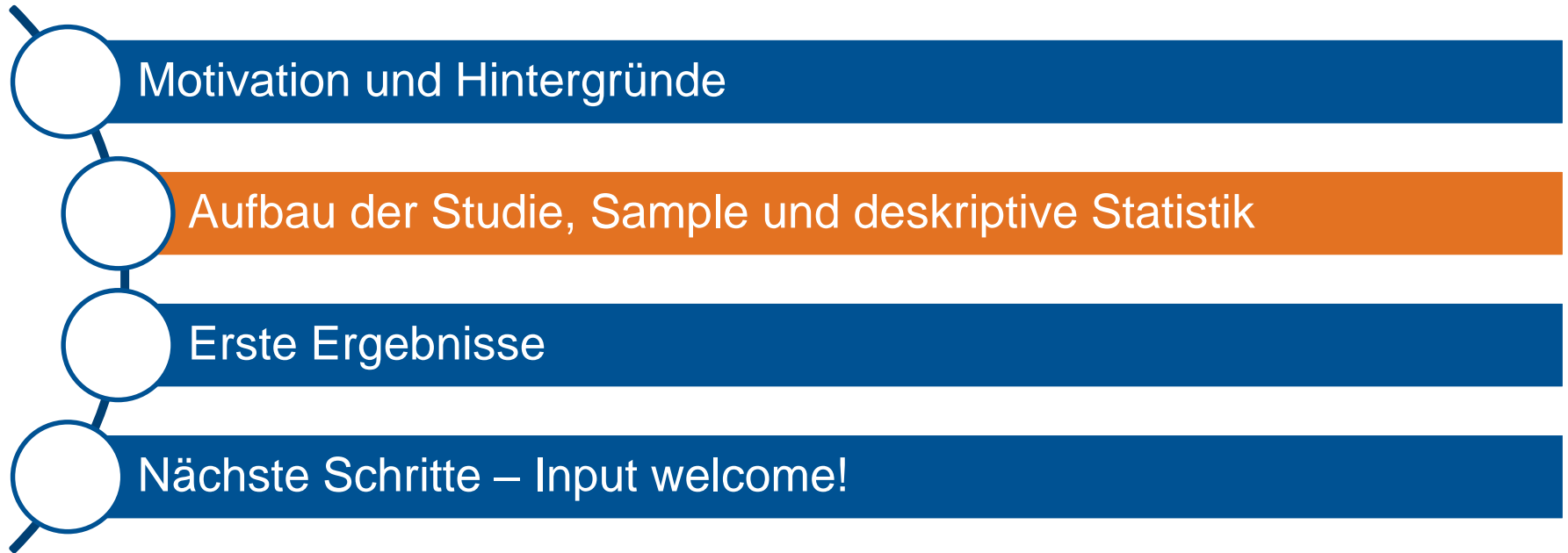
Forschungsfragen



Welche Rolle spielt die OSS Compliance Zertifizierung bei der Auswahl von SW-Lieferanten?

Gibt es Unterschiede in der Wahrnehmung von Selbstzertifizierung und Zertifizierung durch eine Drittpartei?

Agenda



Aufbau der Studie

Criterion	
Previous collaboration with this software supplier	No collaboration Infrequent collaboration Regular collaboration
Software supplier's relevant experience	No experience Little experience Extensive experience
Recommendations from supplier's prior customers	No recommendations Few recommendations Numerous recommendations
Software supplier is ISO certified for OSS compliance	No Yes, through self-certification Yes, through a third party
Total cost of ownership	Below average Average Above average

Which of the two offers would you choose?
(1 of 16)

Software supplier's relevant experience

Recommendations from supplier's prior customers

Software supplier is ISO certified for OSS compliance

Previous collaboration with this software supplier

Total cost of ownership

	Option 1	Option 2	None
<u>Software supplier's relevant experience</u>	No experience	Extensive experience	
<u>Recommendations from supplier's prior customers</u>	Numerous recommendations	Few recommendations	
<u>Software supplier is ISO certified for OSS compliance</u>	No	Yes, through self-certification	I wouldn't choose any of them.
<u>Previous collaboration with this software supplier</u>	Regular collaboration	Infrequent collaboration	
<u>Total cost of ownership</u>	Average	Above average	
	CBCshort_Random1	CBCshort_Random1	CBCshort_Random1

Back

Next

Sample und deskriptive Statistik

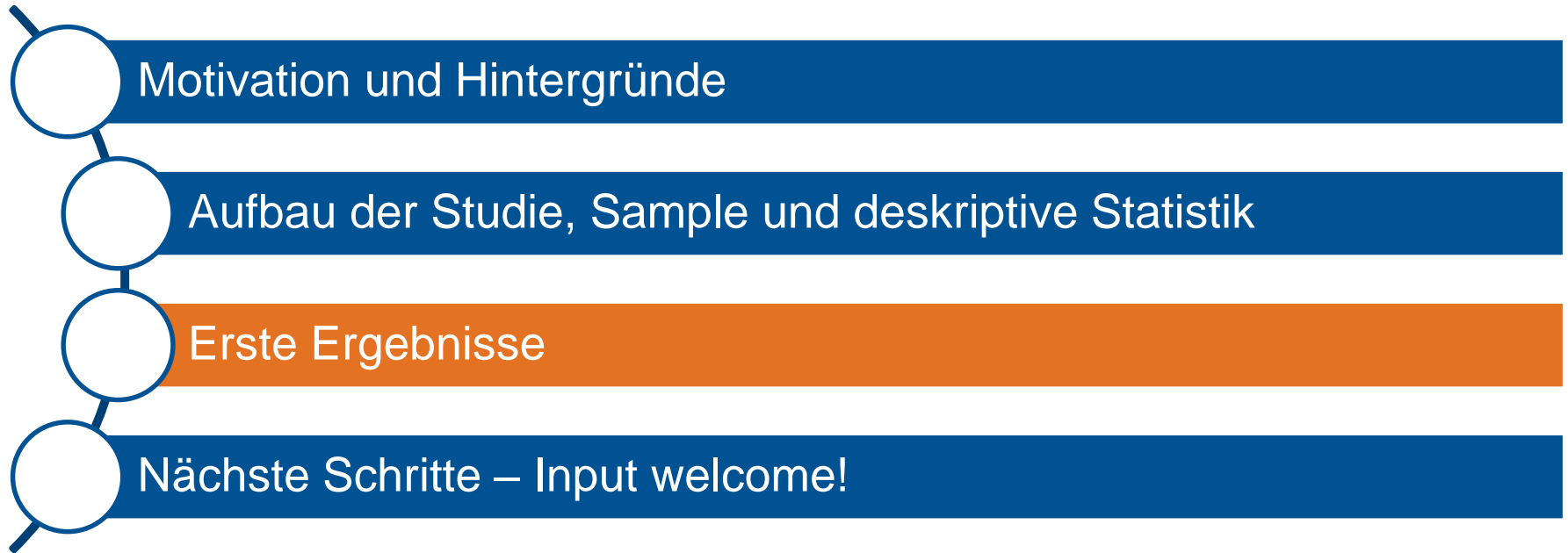
- 82 Teilnehmer
- Studienfach: Computer Sciences, Business Management, Engineering, Law
- Position: Manager, Einkäufer, Technical Specialists, Director
- 76,8% der Firmen in Deutschland
- Industrie: ICT, Manufacturing/Transport/Logistics, Engineering
- Unternehmensgröße: 22,0% weniger als 250 Mitarbeiter

51,2% mehr als 10.000 Mitarbeiter

LocationBU	Freq.	Percent
Austria	2	2.44
Brazil	1	1.22
Denmark	1	1.22
France	1	1.22
Germany	63	76.83
India	4	4.88
Netherlands	1	1.22
South Korea	1	1.22
Switzerland	3	3.66
UK	2	2.44
USA	3	3.66
Total	82	100.00

IndustryBU	Freq.	Percent
Banking/Financial Services	4	4.88
Consulting/Strategy	4	4.88
Engineering	11	13.41
Government/Defense	2	2.44
Healthcare/Medical	4	4.88
ICT	29	35.37
Insurance/Superannuation	1	1.22
Legal	1	1.22
Manufacturing, Transport & Logistics	17	20.73
Marketing/Communications	1	1.22
Mining, Resources & Energy	1	1.22
Retail/Consumer Products	3	3.66
Science/Technology	4	4.88
Total	82	100.00

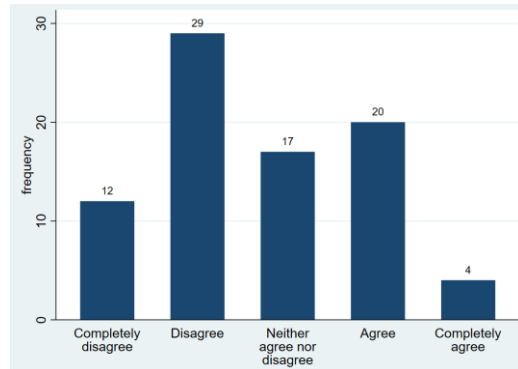
Agenda



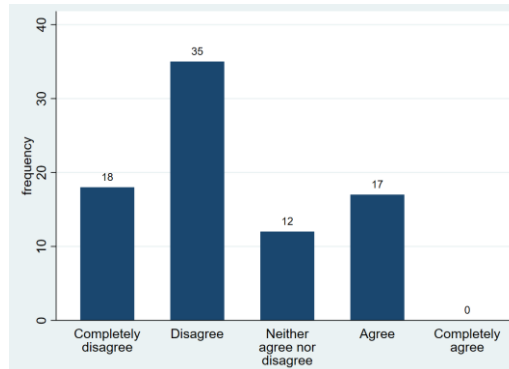
Empfundenes Risiko der OSS Beschaffung

„Die Beschaffung von OSS ist mit einem hohen Risiko verbunden.“

„Insgesamt betrachte ich die Beschaffung von OSS in meiner BU als risikoreich.“



29,3% Zustimmung



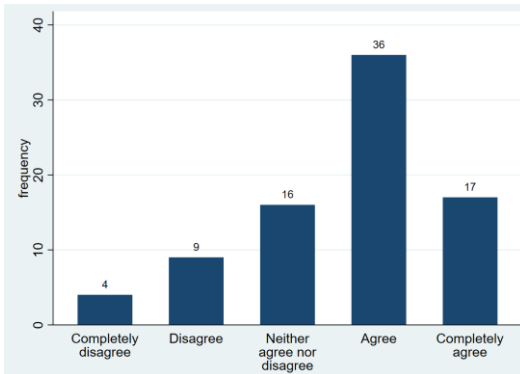
20,7%



25% der Teilnehmer sehen ein Risiko in der Beschaffung von OSS

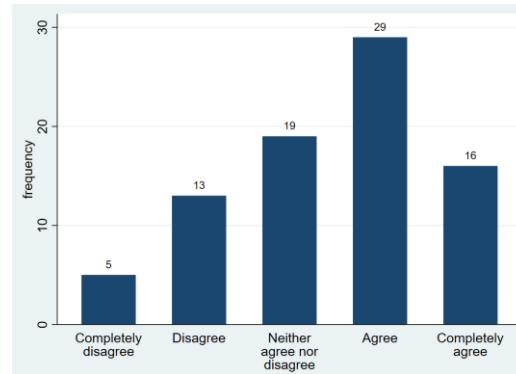
Deep Dive: Worin genau besteht das Risiko?

„Die Nichteinhaltung von OSS Lizenzen führt zu einem erheblichen **Reputationsverlust.**“



64,6% Zustimmung

„Die Nichteinhaltung von OSS Lizenzen führt zu einem erheblichen **finanziellen Verlust.**“



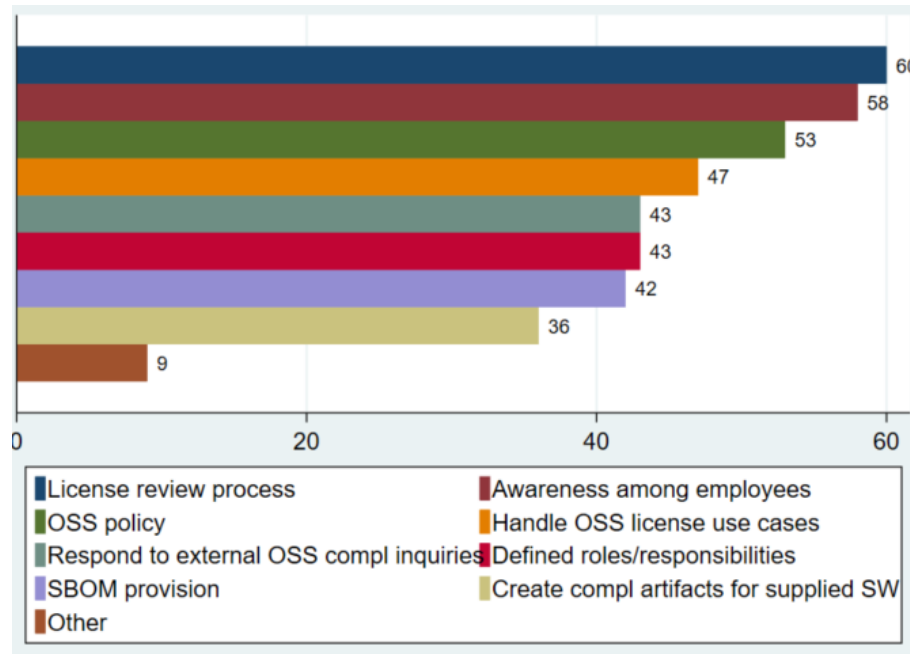
54,9%

Außerdem:

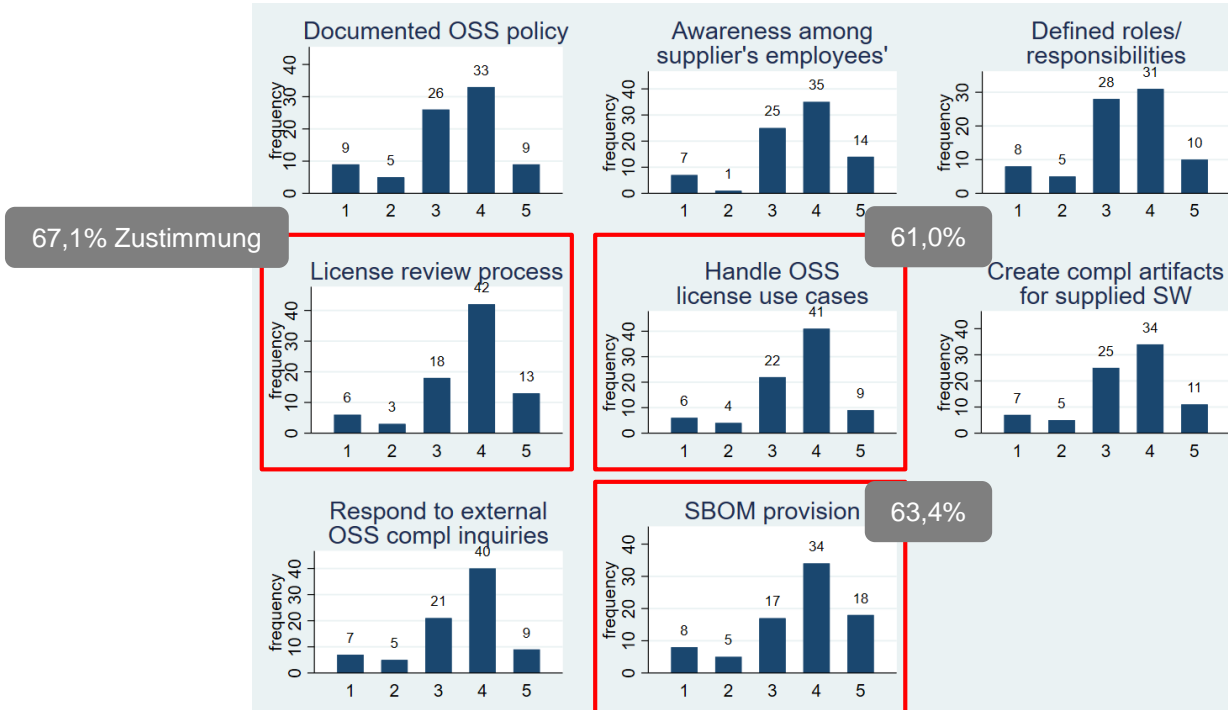
OSS macht meine BU stark **abhängig** von der entsprechenden OSS Community bzw. dem SW-Lieferanten. 47,6%

Der Einsatz von OSS verursacht **unvorhergesehene Kosten.** 29,3%

Welche OSS Compliance Maßnahmen haben Unternehmen etabliert?

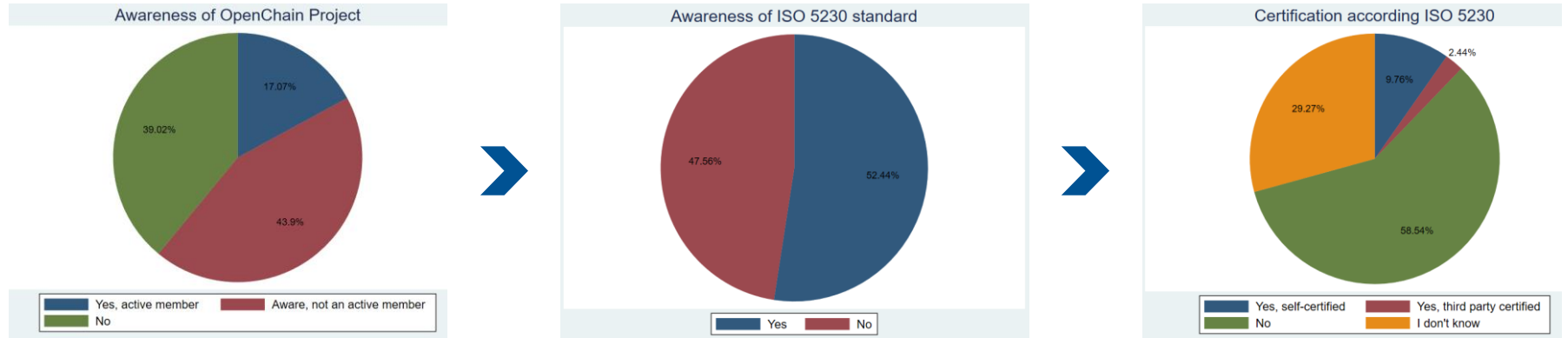


Welche OSS Compliance Maßnahmen sind wichtig bei der Auswahl von SW-Lieferanten?



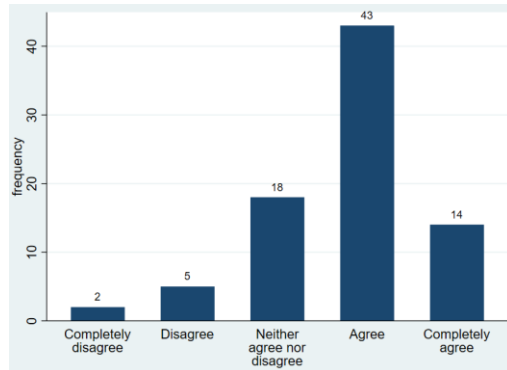
- 1 Completely unimportant
- 2 Unimportant
- 3 Neither important nor unimportant
- 4 Important
- 5 Very important

Bekanntheit des Standards ISO 5230 bzw. des OpenChain Projekts



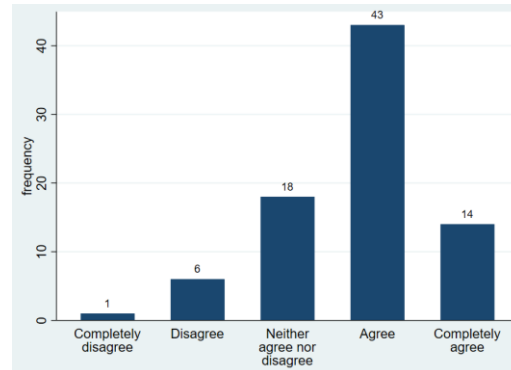
Signalwirkung der OSS Compliance Zertifizierung

„Diese Zertifizierung signalisiert **Vertrauenswürdigkeit.**“



69,5% Zustimmung

„Diese Zertifizierung signalisiert **organisationale Qualität.**“



69,5%

Außerdem:

56,1%

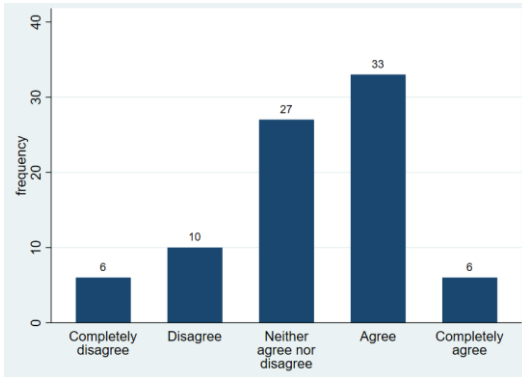
„Diese Zertifizierung signalisiert **Kompetenz.**“

„Diese Zertifizierung signalisiert eine **gute Reputation.**“

56,1%

Treiber für OSS Compliance Zertifizierung

„Diese Zertifizierung hilft Unternehmen, sich **von Wettbewerbern abzuheben.**“



47,6% Zustimmung

35,4%

„Diese Zertifizierung wird von **Kunden** verlangt.“

32,9%

„Diese Zertifizierung wird auf Basis **interner Vorschriften** verlangt.“

34,1%

„Diese Zertifizierung ist eine **gesetzliche** Verpflichtung.“

31,7%

„Diese Zertifizierung ist eine **moralische** Verpflichtung.“

Relevanz verschiedener Faktoren bei der Auswahl von SW-Lieferanten

Average Importances	Average Importances	Standard Deviation
COLLAB	18.77851	8.39926
EXPER	35.02977	11.76209
RECOMM	15.23572	5.78570
CERT	18.71496	12.42411
TCO	12.24104	6.29725



Erfahrung des SW-Lieferanten wichtigstes Entscheidungskriterium,
gefolgt von vorheriger **Zusammenarbeit** bzw. OSS Compliance
Zertifizierung; TCO am wenigsten relevant

Auswirkung versch. Ausprägungen der Faktoren auf die Auswahl von SW-Lieferanten

Variable	qui
decision	
exp_extens~e	2.754***
exp_little	1.162***
col_regular	1.455***
col_infreq~t	0.463**
recom_num~s	0.851***
recom_few	0.418**
cert_third~y	1.235***
cert_self	0.899***
tco_aboveav	-0.864***
tco_average	-0.191
_cons	-3.401***
var(_cons[sys~m])	0.455*



Eine OSS Compliance Zertifizierung hat einen positiven Effekt auf die Auswahl von SW-Lieferanten.

Eine Drittpartei-Zertifizierung ist dabei noch vorteilhafter als eine Selbstzertifizierung (im Vergleich zu keiner Zertifizierung).

Legend: * p<.05; ** p<.01; *** p<.001

Auswirkung der Bekanntheit des ISO 5230 Standards auf die Rolle der OSS Compliance Zertifizierung bei der Auswahl von SW-Lieferanten

Gruppe „Not aware of ISO 5230“

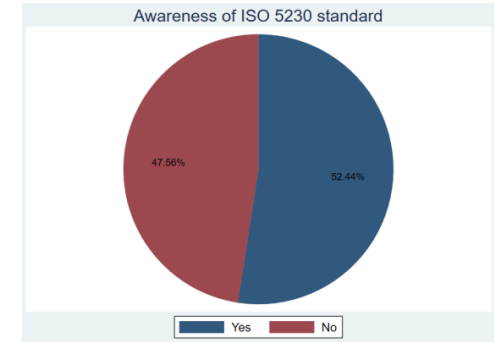
Variable	qui
decision	
exp_extens~e	3.0824823***
exp_little	1.347017***
col_regular	1.3958531***
col_infreq~t	.46654737*
recom_num~s	.82691621***
recom_few	.48352158*
cert_third~y	1.0438268***
cert_self	.50182631*
tco_aboveav	-1.0070448***
tco_average	-.39659885
_cons	-3.2115776***
var(_cons[sys~m])	.34351845

Legend: * p<.05; ** p<.01; *** p<.001

Gruppe „Aware of ISO 5230“

Variable	qui
decision	
exp_extens~e	2.5136252***
exp_little	1.0458425***
col_regular	1.4945981***
col_infreq~t	.40950222*
recom_num~s	.87914849***
recom_few	.37287669
cert_third~y	1.4190096***
cert_self	1.2561646***
tco_aboveav	-.74748287**
tco_average	.02014604
_cons	-3.6180834***
var(_cons[sys~m])	.58729385

Legend: * p<.05; ** p<.01; *** p<.001



Ist der ISO 5230 Standard bekannt, steigt die Bedeutung einer Selbstzertifizierung im Vergleich zu einer Drittparteizertifizierung.

Agenda



Nächste Schritte

- Akquise weiterer Teilnehmer
- Tiefergehende Analysen (z.B. Einfluss von Größe des bezogenen SW-Projekts, Industrie, Bedeutung von OSS für Business Model, Engagement in OSS Communities, Formalisierungsgrad des Jobs, etc.)



Ihr Input ist sehr wertvoll

Herzlichen Dank für Ihre Aufmerksamkeit

Juliane Wissel

juliane.wissel@tum.de

Dr. Theo Schöller-Stiftungslehrstuhl für Technologie- und
Innovationsmanagement
TUM School of Management
Technische Universität München



Link zur Teilnahme an der Studie:

<https://OSSComplianceTUM.sawtoothsoftware.com/login.html>