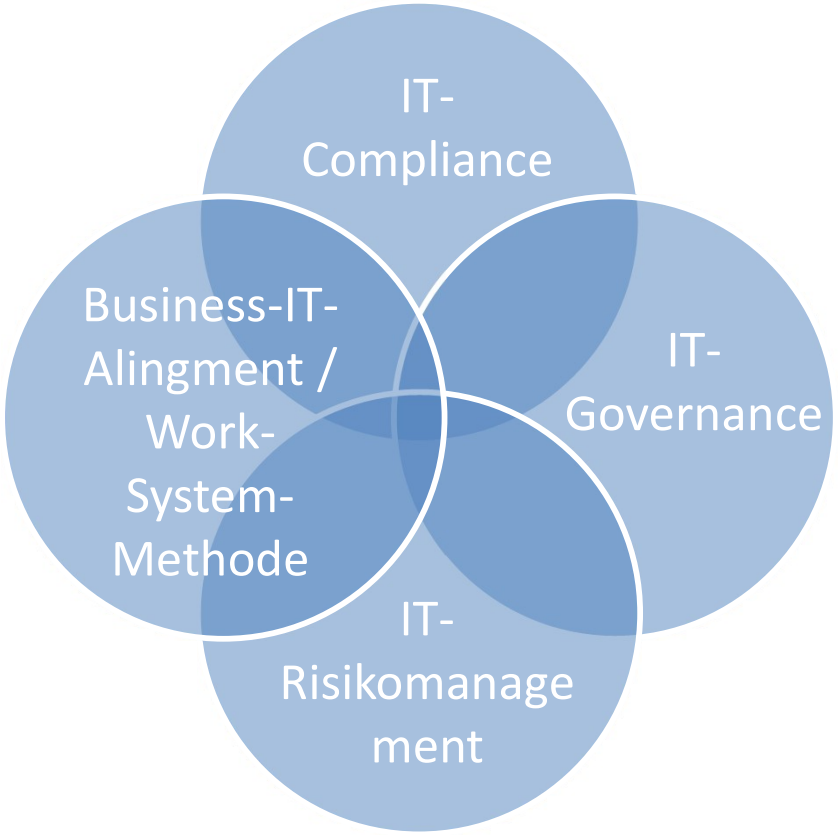
IT - Compliance in KMU

Dr. Nico Deistler

Agenda

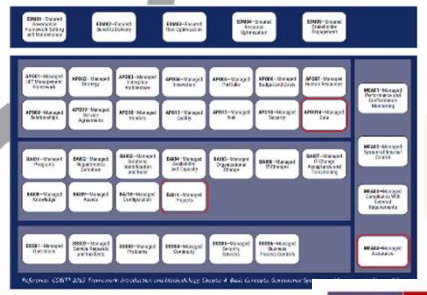
- 1. Problemstellung und Relevanz
- 2. Methodik
  - Identifikation
  - Adaptierung
  - Anwendung
- 3. Ergebnisse und Einordnung

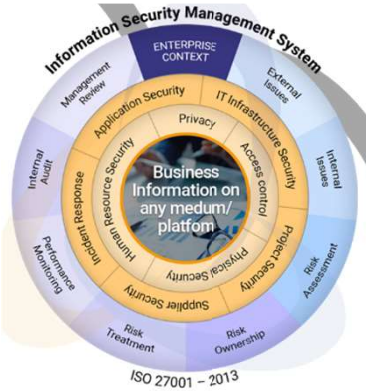
Problemstellung und Relevanz (1/2)



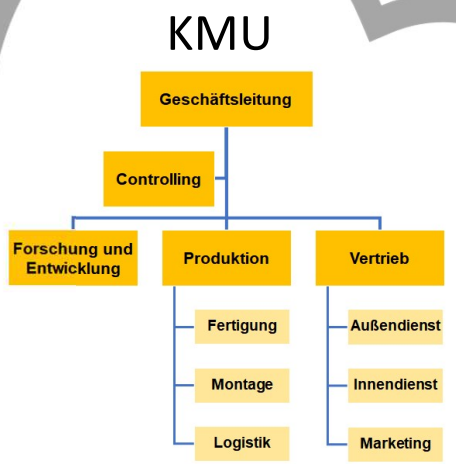
Problemstellung und Relevanz (2/2)

Rahmenwerke





IT- und Organisationsstrukturen



Im Ergebnis drohen **wirtschaftliche Nachteile** in Form von Strafen bei Gesetzesverstößen, Schäden aus IT-Sicherheitsvorfällen und auch Imagenachteile. Es zeigt sich also eine **unmittelbare praktische Relevanz** des Themas.

Methodik

» Methodik zum angepassten Einsatz von Rahmenwerken

<table>
<tr><th>Identifikation</th><th colspan="2">Adaption</th><th>Anwendung</th></tr>
<tr><td rowspan="3">Identifikation des relevanten Rahmenwerkes</td><td>Zuweisung Prozesse und Aktivitäten -> Domäne</td><td rowspan="2">Als Basis dienen die Strukturelemente (Domänen und Work System Methode - Elemente)</td><td rowspan="3">Zuweisung ausgewählter Domänen -> Prozesse und Aktivitäten</td></tr>
<tr><td>Zuweisung Prozesse und Aktivitäten -> WSM (für ausgewählte Domänen aus vorherigem Schritt)</td></tr>
<tr><td>Zuweisung und Rating je Ausprägungskriterium Archetyp -> Domäne</td><td>Als Basis dienen die Archetypen (SME relevante Ausprägungen)</td></tr>
</table>

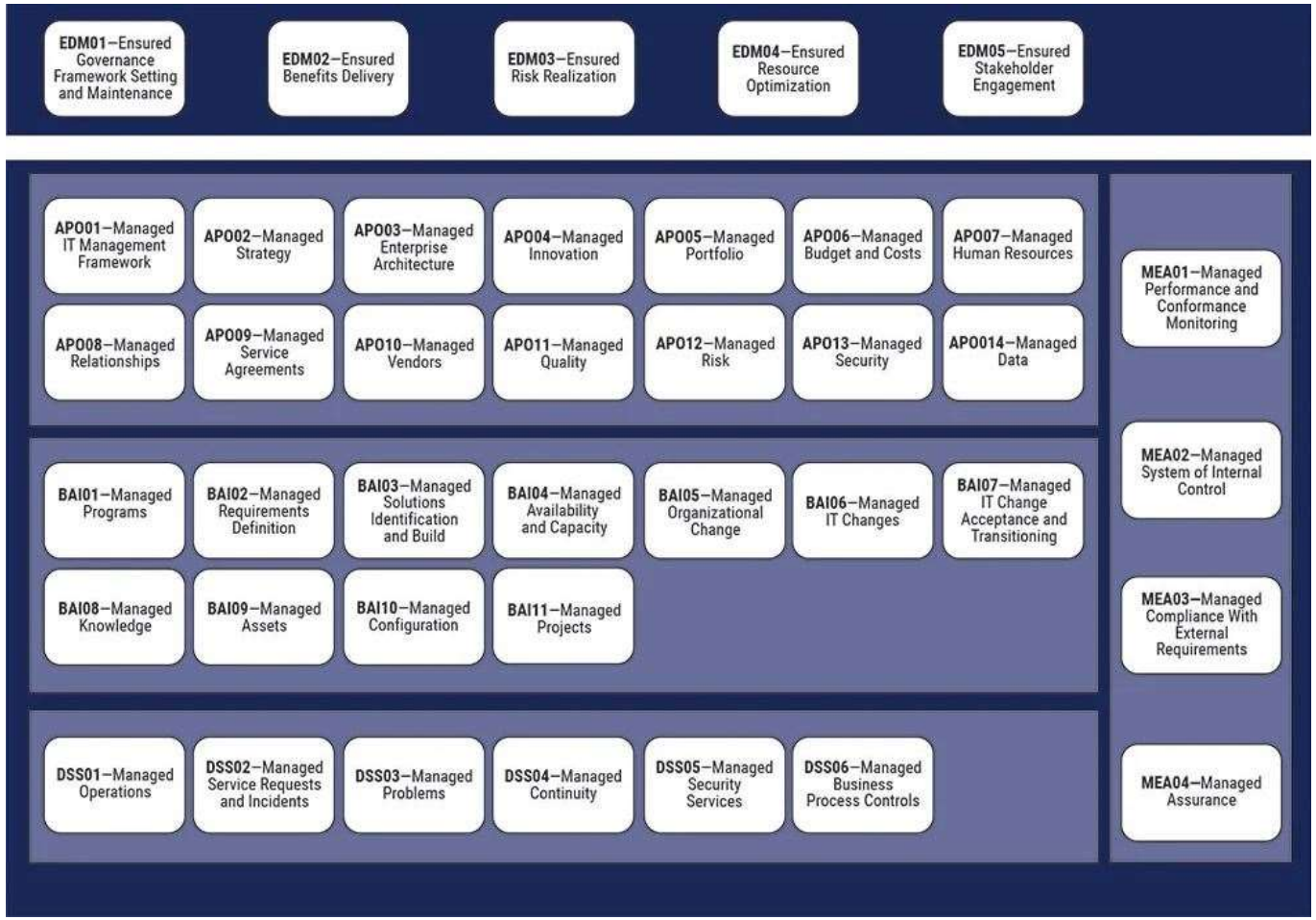
Methodik – Identifikation (1/2)

» Methodik zum angepassten Einsatz von Rahmenwerken

Identifikation	Adaption		Anwendung
Identifikation des relevanten Rahmenwerkes	Zuweisung Prozesse und Aktivitäten -> Domäne	Als Basis dienen die Strukturelemente (Domänen und Work System Methode - Elemente)	Zuweisung ausgewählter Domänen -> Prozesse und Aktivitäten
	Zuweisung Prozesse und Aktivitäten -> WSM (für ausgewählte Domänen aus vorherigem Schritt)		
	Zuweisung und Rating je Ausprägungskriterium Archetyp -> Domäne	Als Basis dienen die Archetypen (SME relevante Ausprägungen)	

Methodik – Identifikation (2/2)

» **Identifikation**: COBIT 2019 Rahmenwerk



Methodik – Adaption (1/3)

» Methodik zum angepassten Einsatz von Rahmenwerken

Identifikation	Adaption		Anwendung
Identifikation des relevanten Rahmenwerkes	Zuweisung Prozesse und Aktivitäten -> Domäne	Als Basis dienen die Strukturelemente (Domänen und Work System Methode - Elemente)	Zuweisung ausgewählter Domänen -> Prozesse und Aktivitäten
	Zuweisung Prozesse und Aktivitäten -> WSM (für ausgewählte Domänen aus vorherigem Schritt)		
	Zuweisung und Rating je Ausprägungskriterium Archetyp -> Domäne	Als Basis dienen die Archetypen (SME relevante Ausprägungen)	

Methodik – Adaption (2/3)

Prozesse und Aktivitäten

Strukturelemente

	IT Principles			Management of IT			Architecture			Sourcing			Security,Risk,Compliance			Organization and Personal			IT Services		
	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T
EDM01 - Ensured Governance Framework setting and Maintenance				n/a			A.5 Information Security Policies, A.6 Organization of Information Security			x	x											
EDM02 - Ensured Benefits Delivery				n/a			A.5 Information Security Policies, A.6 Organization of Information Security			x	x		x	x								
EDM03 - Ensured Risk Optimization				Risk Management			A.5 Information Security Policies, A.6 Organization of Information Security									x	x	x				
EDM04 - Ensured Resource Optimization				n/a			A.5 Information Security Policies, A.6 Organization of Information Security				x		x	x	x					x		
EDM05 - Ensured Stakeholder Engagement				n/a			A.5 Information Security Policies, A.6 Organization of Information Security			x	x											
APO01 - Managed I&T Framework Management				n/a			n/a			x	x	x										
APO02 - Managed Strategy				Strategy Management			n/a			x	x		x	x	x		x		x	x	x	x
APO03 - Managed Enterprise Architecture				Architecture Management			n/a						x	x	x							
APO04 - Managed Innovation				n/a			A.14 System Acquisition, Development and Maintenance				x		x	x			x					
APO05 - Managed Portfolio				Portfolio Management			n/a				x		x	x			x					
APO06 - Managed Budget and Cost				Service financial management			n/a						x	x	x							
APO07 - Managed Human Resources				Workforce and talent management			A.7 Human resource security													x	x	
APO08 - Managed Relationships				Relationship Management			n/a				x									x	x	
APO09 - Managed Service Agreements				Service catalogue management, Service level management			n/a															x	x	x
APO10 - Managed Vendors				Supplier management			A.15 Supplier Relationships															
APO11 - Managed Quality				n/a			n/a				x									x	x	
APO12 - Managed Risk				Risk Management			n/a									x	x					

Methodik – Adaption (3/3)

» Differenzierung von KMUs mithilfe von Archetypen

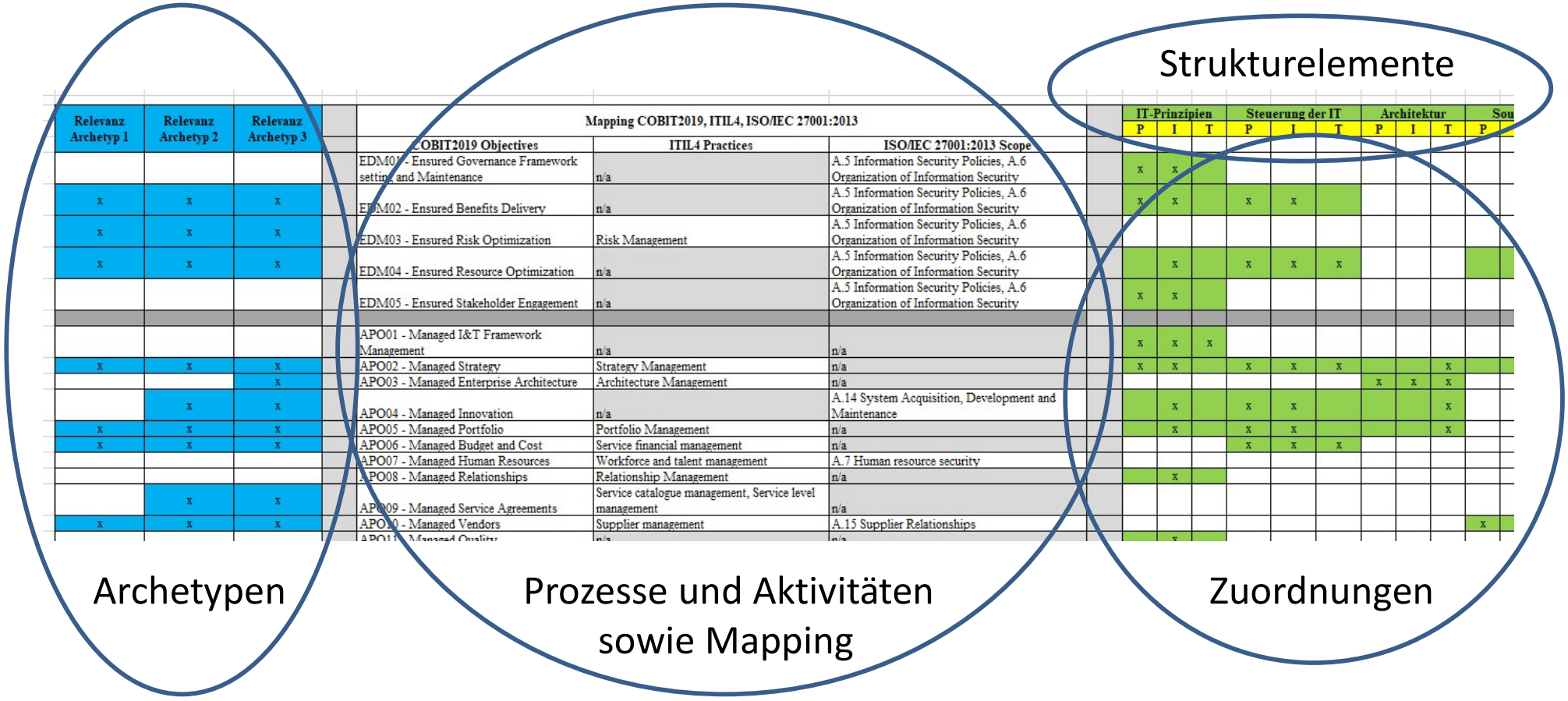
Archetyp	Ausprägungen
1	kleines Unternehmen, IT hauptsächlich ausgelagert, keine klare Verantwortung für die IT, begrenzte interne IT-Kenntnisse/-Kapazitäten, relativ hohe Risikotoleranz aufgrund geringer Risikokapazität, einfache Befehlsstruktur und begrenzte Organisationsstrukturen vorhanden
2	kleines Unternehmen, IT hauptsächlich intern, IT-Abteilung vorhanden, komplexere Aufgaben werden ausgelagert, begrenzte interne IT-Fähigkeiten und/oder -Kapazitäten, relativ hohe Risikotoleranz aufgrund geringer Risikokapazität, einfache Befehlsstruktur und begrenzte Organisationsstrukturen vorhanden
3	mittelgroßes Unternehmen, heterogene IT-Landschaft und IT-Abteilung vorhanden, möchten eher kaufen (und möglicherweise anpassen) als selbst entwickeln, komplexere Aufgaben auslagern

Methodik – Anwendung (1/3)

» Methodik zum angepassten Einsatz von Rahmenwerken

Identifikation	Adaption		Anwendung
Identifikation des relevanten Rahmenwerkes	Zuweisung Prozesse und Aktivitäten -> Domäne	Als Basis dienen die Strukturelemente (Domänen und Work System Methode - Elemente)	Zuweisung ausgewählter Domänen -> Prozesse und Aktivitäten
	Zuweisung Prozesse und Aktivitäten -> WSM (für ausgewählte Domänen aus vorherigem Schritt)		
	Zuweisung und Rating je Ausprägungskriterium Archetyp -> Domäne	Als Basis dienen die Archetypen (SME relevante Ausprägungen)	

Methodik – Anwendung (2/3)



Relevanz Archetyp 1	Relevanz Archetyp 2	Relevanz Archetyp 3	Mapping COBIT2019, ITIL4, ISO/IEC 27001:2013			IT-Prinzipien			Steuerung der IT			Architektur			Sou
			COBIT2019 Objectives	ITIL4 Practices	ISO/IEC 27001:2013 Scope	P	I	T	P	I	T	P	I	T	P
			EDM01 - Ensured Governance Framework setting and Maintenance	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x								
x	x	x	EDM02 - Ensured Benefits Delivery	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x		x	x					
x	x	x	EDM03 - Ensured Risk Optimization	Risk Management	A.5 Information Security Policies, A.6 Organization of Information Security										
x	x	x	EDM04 - Ensured Resource Optimization	n/a	A.5 Information Security Policies, A.6 Organization of Information Security		x		x	x	x				
			EDM05 - Ensured Stakeholder Engagement	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x								
			APO01 - Managed I&T Framework Management	n/a	n/a	x	x	x							
x	x	x	APO02 - Managed Strategy	Strategy Management	n/a	x	x		x	x	x			x	
		x	APO03 - Managed Enterprise Architecture	Architecture Management	n/a							x	x	x	
	x	x	APO04 - Managed Innovation	n/a	A.14 System Acquisition, Development and Maintenance		x		x	x				x	
x	x	x	APO05 - Managed Portfolio	Portfolio Management	n/a		x		x	x				x	
x	x	x	APO06 - Managed Budget and Cost	Service financial management	n/a				x	x	x				
			APO07 - Managed Human Resources	Workforce and talent management	A.7 Human resource security										
			APO08 - Managed Relationships	Relationship Management	n/a		x								
	x	x	APO09 - Managed Service Agreements	Service catalogue management, Service level management	n/a										
x	x	x	APO10 - Managed Vendors	Supplier management	A.15 Supplier Relationships										x
			APO11 - Managed Quality	n/a	n/a		x								

Zuordnungen im Ausgangszustand: Personal (47), Information (42) und Technology (33)

Archetyp 1: Personal (22), Information (22) und Technology (15)

Archetyp 2: Personal (34), Information (29) und Technology (29)

Archetyp 3: Personal (40), Information (33) und Technology (32)

Methodik – Anwendung (3/3)

Relevanz Archetyp 1	Relevanz Archetyp 2	Relevanz Archetyp 3	Mapping COBIT2019, ITIL4, ISO/IEC 27001:2013			IT-Prinzipien			Steuerung der IT			Architektur			Sourcing			Security,Risk,Compliance			Organisation & Personal			IT Services		
						P	I	T	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T	P	I	T
			COBIT2019 Objectives	ITIL4 Practices	ISO/IEC 27001:2013 Scope																					
			EDM01 - Ensured Governance Framework setting and Maintenance	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x																			
x	x	x	EDM02 - Ensured Benefits Delivery	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x		x	x																
x	x	x	EDM03 - Ensured Risk Optimization	Risk Management	A.5 Information Security Policies, A.6 Organization of Information Security													x	x	x						
x	x	x	EDM04 - Ensured Resource Optimization	n/a	A.5 Information Security Policies, A.6 Organization of Information Security		x		x	x	x						x				x					
			EDM05 - Ensured Stakeholder Engagement	n/a	A.5 Information Security Policies, A.6 Organization of Information Security	x	x																			
			APO01 - Managed I&T Framework Management	n/a	n/a	x	x	x																		
x	x	x	APO02 - Managed Strategy	Strategy Management	n/a		x			x	x	x				x					x	x	x	x				x
		x	APO03 - Managed Enterprise Architecture	Architecture Management	n/a								x	x	x												
	x	x	APO04 - Managed Innovation	n/a	A.14 System Acquisition, Development and Maintenance		x		x	x						x										
x	x	x	APO05 - Managed Portfolio	Portfolio Management	n/a		x		x	x						x										
x	x	x	APO06 - Managed Budget and Cost	Service financial management	n/a				x	x	x																
			APO07 - Managed Human Resources	Workforce and talent management	A.7 Human resource security																x	x					
			APO08 - Managed Relationships	Relationship Management	n/a		x														x	x					
	x	x	APO09 - Managed Service Agreements	Service catalogue management, Service level management	n/a																			x	x	x
x	x	x	APO10 - Managed Vendors	Supplier management	A.15 Supplier Relationships										x	x										
			APO11 - Managed Quality	n/a	n/a		x														x	x					
x	x	x	APO12 - Managed Risk	Risk Management	n/a													x	x							
x	x	x	APO13 - Managed Security	Information security management	A.14 System Acquisition, Development and Maintenance, A.18 Compliance													x	x							
		x	APO14 - Managed Data	Business analysis	A.12 Operations security, A.14 System Acquisition, Development and Maintenance							x	x	x												
		x	BAI01 - Managed Programs	Portfolio Management	n/a																x	x		x		x
	x	x	BAI02 - Managed Requirements Definition	Business analysis, Service design, Service level management	n/a																			x	x	
	x	x	BAI03 - Managed Solutions Identification and Build	Service design, Software development and management	n/a																				x	x
	x	x	BAI04 - Managed Availability and Capacity	Capacity and performance management, Availability Management	n/a																			x		x
	x	x	BAI05 - Managed Organizational Change	Organizational change management	n/a																			x		
	x	x	BAI06 - Managed IT Changes	Change enablement	n/a																			x		x
	x	x	BAI07 - Managed IT Change Acceptance and Transitioning	Release Management, Service validation and testing, Deployment management	n/a																			x		x
			BAI08 - Managed Knowledge	Knowledge Management	n/a																x	x				
	x	x	BAI09 - Managed Assets	IT asset management	A.8 Asset management									x												x
	x	x	BAI10 - Managed Configuration	Service configuration management	n/a									x										x	x	x
		x	BAI11 - Managed Projects	Project Management	n/a																x	x		x		
	x	x	DSS01 - Managed Operations	Monitoring and event management, Infrastructure and platform management	A.12 Operations security																			x		x
	x	x	DSS02 - Manage Service Requests and Incidents	Incident management, Service desk, Service request management	n/a																			x		x
	x	x	DSS03 - Managed Problems	Problem Management	n/a																			x		x
	x	x	DSS04 - Managed Continuity	Service continuity management	A.17 Information security aspects of Business Continuity Management																			x	x	x
x	x	x	DSS05 - Managed Security Services	Information security management	A.9 Access control, A.10 Cryptography, A.11 Physical and Environmental Security, A.12 Operations security, A.13 Communication Security, A.16 Information security incident management														x	x	x	x		x			x
x	x	x	DSS06 - Managed Business Process Controls	n/a	n/a													x		x						x
x	x	x	MEA01 - Managed Performance and Conformance Monitoring	Measurement and reporting	n/a		x		x	x	x							x		x						
x	x	x	MEA02 - Managed System of Internal Control	n/a	n/a													x	x							
x	x	x	MEA03 - Managed Compliance with external Requirements	n/a	A.18 Compliance													x	x							
x	x	x	MEA04 - Managed Assurance	n/a	A.12 Operations security													x	x							

Ergebnisse und Einordnung (1/2)

- Die Methode hat die Fähigkeit, die Entscheidung zur Auswahl von Aktivitäten zu **objektivieren** und zu **systematisieren**.

- Management kann **zielgerichteter** auf Basis der Organisationsstruktur handeln und damit die (fehlenden) Kapazitäten effizienter einsetzen

- Ansatz mit **Gewichtung des Ressourcenbedarfs**, der Kosten-Nutzen Relation ermöglicht

Ergebnisse und Einordnung (2/2)

» **Fehlende spezifische** und **umsetzbare Lösungen für KMU** aus der Literatur wurde aufgegriffen und eine **Vorgehensweise** auf der **vorhandenen Wissensbasis** erstellt.

IT-Governance	• Mithilfe der Methode werden dem Management Optionen und damit eine Handlungsoption der Integration bereitgestellt.
IT-Risikomanagement	• Security- und Cyber-relevante Themen werden in der Methodik als wichtig eingestuft, die damit besonders priorisiert und zu einer höheren Anwendung führen.
Business-IT-Alignment/Work-System-Methode	• Ergänzt mit den Ansätzen der Work-System-Methode wird auf die spezifischen Anforderungen in KMU wie Personal, Information und Technologie eingegangen.
IT-Compliance Ansätzen	• Entgegen der bisherigen primär grundlegenden Ausrichtung der Forschung konzentriert sich diese Arbeit auf die Konkretisierung von bereits vorhandenen Ansätzen.

Vielen Dank – Fragen gerne …

Kontakt unter:

- ERP-Kompetenzzentrum – FH Kufstein Tirol
- ERP-Kompetenzzentrum: LinkedIn