ANHANG 17-G

FRAGENKATALOG ZU NACHWEISEN INTERNATIONALER NORMEN UND ZERTIFIZIERUNGEN

Stand November 2017

INHALTSVERZEICHNIS

Ref #	Anforderungen der MAN	Erfüllt (ja, nein)	Kommentar
1.0	**EINFÜHRUNG (KONFORMITÄTSANFORDERUNGEN AN DIE MANAGEMENTPRAKTIKEN DES AN)**		
	Die Leitlinien, Managementsysteme, Prozesse, praktische Verfahren und Maßnahmen der MAN basieren u.a. auf den international gültigen Standards ISO/IEC 9001, ISO/IEC 14001, SA8000, OHS-AS 18001, OHS-AS 18002, ITL V3, ISO/IEC 20000-1, ISO/IEC 27001, ISO/IEC 31000, ISO/IEC 27005 und ISO/IEC 24762. Die implementierten Leitlinien und Managementsysteme dienen dazu, die effektive Planung, das Management, die Kontrolle und die Performance der Produkt- oder Servicequalität sicher zu stellen. Die Managementsysteme folgen dem Prinzip der kontinuierlichen Verbesserung und ständigen Optimierung nach der PDCA-Methodik (Plan-Do-Check-Act). Das Management des ANs ist verpflichtet, dass diese Leitlinien in allen betroffenen Bereichen der Organisation, die für die Leistungserfüllung an MAN benötigt werden, kommuniziert, verstanden und umgesetzt werden.		
2.0	**INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM (ISMS) — ISO/IEC 27001**		
Anh.17-G – 1.	1. Der AN hat Leitlinien zur Informationssicherheit und Vertraulichkeit für alle seine Organisationsbereiche implementiert, die definieren, wie der AN Risiken in Bezug auf Informationssicherheit handhabt.		
Anh.17-G – 2.	2. Der AN sichert zu, dass seine Informationssicherheits-Managementpraxis, die bei der Unterstützung der *Services* zur Anwendung kommt, auf dem aktuellen Standard ISO 27001 basiert		
Anh.17-G – 3.	3. Der AN hat ein *Informationssicherheits-Managementsystem (ISMS)* für alle Geschäftsbereiche, die zur Leistungserbringung an MAN benötigt werden, etabliert, das gemäß ISO/IEC 27001:2016 zertifiziert ist		
	4. Das Managementsystem folgt dem Prinzip der kontinuierlichen Verbesserung und ständigen Optimierung nach der PDCA-Methodik (Plan-Do-Check-Act).		
Anh.17-G – 4.	5. Erfahrungen aus der Vergangenheit werden verwendet, um Risiken zu minimieren und das Managementsystem zu verbessern		

Ref #	Anforderungen der MAN	Erfüllt (ja, nein)	Kommentar
3.0	**SECURITY INCIDENT MANAGEMENT — ISO18044**		
Anh.17-G – 5.	1. Der AN hat ein dokumentiertes Security *Incident Management* etabliert, in der explizit beschrieben ist, welche Regeln / Prozeduren zur systematischen Erkennung, Evaluierung, Behandlung, Dokumentation, Reporting und Bewertung von Sicherheitsvorfällen im Unternehmen angewendet werden, und welche präventive Maßnahmen zur Verhinderung von Security *Incidents* umgesetzt werden.		
Anh.17-G – 6.	2. Die Maßnahmen sind abhängig von verschiedenen Stufen eines Sicherheitsvorfalls		
Anh.17-G – 7.	3. Es sind Leitlinien für die Identifizierung und Implementierung notwendiger technischer, organisatorischer Maßnahmen und Verfahren zur Behebung oder zum Ausschluss von Sicherheitsvorfällen vorhanden		
Anh.17-G – 8.	4. Das Management sorgt dafür diese Leitlinien regelmäßig in allen Bereichen der Organisation kommuniziert, verstanden und umgesetzt werden		
Anh.17-G – 9.	5. Das dokumentiertes Security *Incident Management* folgt den Richtlinien der ISO/IEC TR 18044:2004 (zukünftig ISO/IEC 27035)		
Anh.17-G – 10.	6. Das Managementsystem folgt dem Prinzip der kontinuierlichen Verbesserung und ständigen Optimierung nach der PDCA-Methodik (Plan-Do-Check-Act)		
Anh.17-G – 11.	7. Erfahrungen aus der Vergangenheit werden verwendet, um Risiken zu minimieren und das Managementsystem zu verbessern		
4.0	**RISIKO-MANAGEMENT ISO/IEC 27005 UND ISO/IEC 31000**		
Anh.17-G – 12.	1. Der AN hat Leitlinien, Anweisungen, Verfahren und Maßnahmen zur systematischen Erkennung, Analyse, Bewertung, Überwachung und Kontrolle von Risiken für alle seine Kernkompetenzen und Aktivitäten, die zur Aufrechterhaltung seines Geschäftsbetriebs und seiner Geschäftsverbindungen gefordert sind, etabliert.		

Ref #	Anforderungen der MAN	Erfüllt (ja, nein)	Kommentar
Anh.17-G – 13.	2. Seine Anwendungsbereiche sind u. a. Unternehmensrisiken, Umweltrisiken (z.B. Sturm, Hochwasser), Technische Risiken, Produktrisiken, *Software*-Risiken, etc.		
Anh.17-G – 14.	3. Das Management sorgt dafür, dass diese Leitlinien regelmäßig in allen Bereichen der Organisation kommuniziert, verstanden und umgesetzt werden		
Anh.17-G – 15.	4. Das Risiko-Management folgt den Richtlinien der ISO/IEC 31000:2009 und der ISO/IEC 27005:2011 Information Security Risk Management		
Anh.17-G – 16.	5. Das Managementsystem folgt dem Prinzip der kontinuierlichen Verbesserung und ständigen Optimierung nach der PDCA-Methodik (Plan-Do-Check-Act)		
Anh.17-G – 17.	6. Erfahrungen aus der Vergangenheit werden verwendet, um Risiken zu minimieren und das Managementsystem zu verbessern		
5.0	**SICHERSTELLEN DES GESCHÄFTSBETRIEBS (BUSINESS CONTINUITY // IT-DISASTER RECOVERY— ISO/IEC 24762)**		
Anh.17-G – 18.	1. Der AN hat Leitlinien, Anweisungen, Verfahren und Maßnahmen eingeführt, dass die • die IT-*Infrastruktur* sowie • die Telekommunikationseinrichtungen • hinsichtlich des konkreten Schutzbedarfs adäquat darauf eingerichtet ist, einen *Katastrophenfall* bzw. Sicherheitsvorfall zu überstehen und schnellstmöglich den Betrieb wieder aufnehmen zu können. Da typischerweise die IT-*Infrastruktur* für wesentliche Prozesse innerhalb eines Unternehmens essentiell ist, ist es wichtig, die Ausfallzeiten zu minimieren		
Anh.17-G – 19.	2. Das Management sorgt dafür diese Leitlinien regelmäßig in allen Bereichen der Organisation kommuniziert, verstanden und umgesetzt werden.		
Anh.17-G – 20.	3. Das Management sorgt dafür das funktionierende und getestete Notfallpläne für *Disaster* Recovery existieren		

Ref #	Anforderungen der MAN	Erfüllt (ja, nein)	Kommentar
Anh.17-G – 21.	4. Das Design und die Effektivität des Business Continuity Managments des AN wird durch einen regelmäßig erstellten ISAE3000 Bericht sichergestellt.		
Anh.17-G – 22.	5. Die Leitlinien zur I für das IT *Disaster* Recovery folgen den Richtlinien der ISO/IEC 24762 :2008 (Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services) und haben einen Bezug zum *Informationssicherheits-Managementsystem* gemäß ISO/IEC 27001		
Anh.17-G – 23.	6. Das Managementsystem folgt dem Prinzip der kontinuierlichen Verbesserung und ständigen Optimierung nach der PDCA-Methodik (Plan-Do-Check-Act)		
Anh.17-G – 24.	7. Erfahrungen aus der Vergangenheit werden verwendet, um Risiken zu minimieren und das Managementsystem zu verbessern		