APPENDIX 17-G

CHECKLIST TO EVIDENCE INTERNATIONAL NORMS AND CERTIFICATION

November 2017

CONTENTS

Ref no.	MAN requirements	Complied with (yes, no)	Comment
1.0	**INTRODUCTION (CONFORMITY REQUIREMENTS FOR THE CONTRACTOR'S MANAGEMENT PRACTICES)**		
	The MAN guidelines, management systems, processes, practical procedures, and measures are based, amongst others, on 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, and ISO/IEC 24762, all of which are standards valid internationally. The guidelines and management systems that have been implemented serve to ensure effective planning, management, control, and performance of product or service quality. The management systems follow the principle of continuous improvement and constant optimization in line with the PDCA method (plan-do-check-act). The Contractor is obliged to perform its management in a way that means that these guidelines are communicated, understood, and implemented across all affected areas of the organization that are required for the performance of services for MAN.		
2.0	**INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) – ISO/IEC 27001**		
Appendix 17-G – 1.	1. The Contractor has implemented guidelines for information security and confidentiality across all of its organizational areas, with said guidelines defining how the Contractor deals with information security risks.		
Appendix 17-G – 2.	2. The Contractor assures that the information security management practices it uses to support the provision of *services* is based on the latest ISO 27001 standard.		
Appendix 17-G – 3.	3. The Contractor has set up an *Information Security Management System (ISMS)* for all business units required for the performance of services for MAN, with the ISMS in question certified it in accordance with ISO/IEC 27001:2016.		
	4. The Management System follows the principle of continuous improvement and constant optimization in line with the PDCA method (plan-do-check-act).		
Appendix 17-G – 4.	5. Past experience is used to minimize risks and improve the Management System.		
3.0	**SECURITY INCIDENT MANAGEMENT — ISO18044**		
Appendix 17-G – 5.	1. The Contractor has set up Security *Incident Management* that is documented and explicitly outlines which rules / procedures are used to systematically identify, evaluate, deal with,		

Ref no.	MAN requirements	Complied with (yes, no)	Comment
	document, report on, and assess security incidents within the company, as well as which measures are implemented to prevent security *incidents*.		
Appendix 17-G – 6.	2. The measures depend on the different categories of a security incident.		
Appendix 17-G – 7.	3. There are guidelines for identifying and implementing necessary technical and organizational measures and procedures to remedy security incidents or rule them out altogether.		
Appendix 17-G – 8.	4. The Management ensures that these guidelines are communicated, understood, and implemented within all areas of the organization on a regular basis.		
Appendix 17-G – 9.	5. The Security *Incident Management* is documented and follows the guidelines set out under ISO/IEC TR 18044:2004 (in the future: ISO/IEC 27035).		
Appendix 17-G – 10.	6. The Management System follows the principle of continuous improvement and constant optimization in line with the PDCA method (plan-do-check-act).		
Appendix 17-G – 11.	7. Past experience is used to minimize risks and improve the Management System.		
4.0	**RISK MANAGEMENT ISO/IEC 27005 AND ISO/IEC 31000**		
Appendix 17-G – 12.	1. The Contractor has set up guidelines, instructions, procedures, and measures to systematically identify, analyze, evaluate, supervise, and control risks across all its core competencies and activities required in order to maintain its business operations and business connections.		
Appendix 17-G – 13.	2. Its areas of application include company risks, environmental risks (e.g., storm, flooding), technical risks, product risks, *software* risks, etc.		
Appendix 17-G – 14.	3. The Management takes care to ensure that these guidelines are communicated, understood, and implemented within all areas		

Ref no.	MAN requirements	Complied with (yes, no)	Comment
	of the organization on a regular basis.		
Appendix 17-G – 15.	4. The Risk Management follows the guidelines set out under ISO/IEC 31000:2009 and ISO/IEC 27005:2011 Information Security Risk Management.		
Appendix 17-G – 16.	5. The Management System follows the principle of continuous improvement and constant optimization in line with the PDCA method (plan-do-check-act).		
Appendix 17-G – 17.	6. Past experience is used to minimize risks and improve the Management System.		
5.0	**ENSURING BUSINESS CONTINUITY (BUSINESS CONTINUITY // IT DISASTER RECOVERY— ISO/IEC 24762)**		
Appendix 17-G – 18.	1. The Contractor has introduced guidelines, instructions, procedures, and measures which ensure that • the IT *infrastructure* and • telecommunication equipment • are configured in a way that means they can withstand a catastrophe or a security incident and the Contractor can resume operations as quickly as possible in light of the specific need for protection. Since IT *infrastructure* normally tends to be essential for key processes within a company, it is important to keep downtimes to a minimum.		
Appendix 17-G – 19.	2. The Management ensures that these guidelines are communicated, understood, and implemented within all areas of the organization on a regular basis.		
Appendix 17-G – 20.	3. The Management ensures that there are contingency plans for *disaster* recovery that work and have been tested.		
Appendix 17-G – 21.	4. The design and effectiveness of the Contractor's Business Continuity Management are guaranteed as a result of an ISAE3000 report drawn up on a regular basis.		
Appendix 17-G – 22.	5. The guidelines for IT *disaster* recovery follow the guidelines set out under ISO/IEC 24762		

Ref no.	MAN requirements	Complied with (yes, no)	Comment
	:2008 (Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services) and are linked to the Information Security Management System pursuant to ISO/IEC 27001		
Appendix 17-G – 23.	6. The Management System follows the principle of continuous improvement and constant optimization in line with the PDCA method (plan-do-check-act).		
Appendix 17-G – 24.	7. Past experience is used to minimize risks and improve the Management System		