Guide for the Assessment of Marine and Offshore Cyber Security Risks

Effective from 1 January 2018

Emirates Classification Society (Tasneef)
Aldar HQ 19th Floor,
Al Raha Beach, Abu Dhabi, UAE
Abu Dhabi, United Arab Emirates

Phone (+971) 2 692 2333
Fax (+971) 2 445 433
P.O. Box. 111155
info@tasneef.ae

GENERAL CONDITIONS

Definitions:

"*Administration*" means the Government of the State whose flag the Ship is entitled to fly or under whose authority the Ship is authorised to operate in the specific case.

"IACS" means the International Association of Classification Societies.

"*Interested Party*" means the party, other than the Society, having an interest in or responsibility for the Ship, product, plant or system subject to classification or certification (such as the owner of the Ship and his representatives, the ship builder, the engine builder or the supplier of parts to be tested) who requests the Services or on whose behalf the Services are requested.

"*Owner*" means the registered owner, the ship owner, the manager or any other party with the responsibility, legally or contractually, to keep the ship seaworthy or in service, having particular regard to the provisions relating to the maintenance of class laid down in Part A, Chapter 2 of the Rules for the Classification of Ships or in the corresponding rules indicated in the specific Rules.

"Rules" in these General Conditions means the documents below issued by the Society:

(i) Rules for the Classification of Ships or other special units;
(ii) Complementary Rules containing the requirements for product, plant, system and other certification or containing the requirements for the assignment of additional class notations;
(iii) Rules for the application of statutory rules, containing the rules to perform the duties delegated by Administrations;
(iv) Guides to carry out particular activities connected with Services;
(v) Any other technical document, as for example rule variations or interpretations.

"*Services*" means the activities described in Article 1 below, rendered by the Society upon request made by or on behalf of the Interested Party.

"Ship" means ships, boats, craft and other special units, as for example offshore structures, floating units and underwater craft.

"*Society*" or *"TASNEEF"* means Tasneef and/or all the companies in the Tasneef Group which provide the Services.

"*Surveyor*" means technical staff acting on behalf of the Society in performing the Services.

Article 1

1.1. The purpose of the Society is, among others, the classification and certification of ships and the certification of their parts and components. In particular, the Society:
(i) sets forth and develops Rules;
(ii) publishes the Register of Ships;
(iii) issues certificates, statements and reports based on its survey activities.

1.2. The Society also takes part in the implementation of national and international rules and standards as delegated by various G overnments.

1.3. The Society carries out technical assistance activities on request and provides special services outside the scope of classification, which are regulated by these general conditions, unless expressly excluded in the particular contract.

Article 2

2.1. The Rules developed by the Society reflect the level of its technical knowledge at the time they are published. Therefore, the Society, although committed also through its research and development services to continuous updating of the Rules, does not guarantee the Rules meet state-of-the-art science and technology at the time of publication or that they meet the Society's or others' subsequent technical developments.

2.2. The Interested Party is required to know the Rules on the basis of which the Services are provided. With particular reference to Classification Services, special attention is to be given to the Rules concerning class suspension, withdrawal and reinstatemen t. In case of doubt or inaccuracy, the Interested Party is to promptly contact the Society for clarification.
The Rules for Classification of Ships are published on the Society's website: www.tasneef.ae.

2.3. The Society exercises due care and skill:
(i) in the selection of its Surveyors
(ii) in the performance of its Services, taking into account the level of its technical knowledge at the time the Services are performed.

2.4. Surveys conducted by the Society include, but are not limited to, visual inspection and non-destructive testing. Unless otherwise required, surveys are conducted through sampling techniques and do not consist of comprehensive verification or monitoring of the Ship or of the items subject to certification. The surveys and checks made by the Society on board ship do not necessarily require the constant and continuous presence of the Surveyor. The Society may also commission laboratory testing, underwater inspection and other checks carried out by and under the responsibility of qualified service suppliers. Survey practices and procedures are selected by the Society based on its experience and knowledge and according to generally accepted technical standards in the sector.

Article 3

3.1. The class assigned to a Ship, like the reports, statements, certificates or any other document or information issued by the Society, reflects the opinion of the Society concerning compliance, at the time the Service is provided, of the Ship or product subject to certification, with the applicable Rules (given the intended use and within the relevant time frame).
The Society is under no obligation to make statements or provide information about elements or facts which are not part of th e specific scope of the Service requested by the Interested Party or on its behalf.

3.2. No report, statement, notation on a plan, review, Certificate of Classification, document or information issued or given as p art of the Services provided by the Society shall have any legal effect or implication other than a representation that, on the basis of the checks made by the Society, the Ship, structure, materials, equipment, machinery or any other item covered by such document or information meet the Rules. Any such document is issued solely for the use of the Society, its committees and clients or other duly authorised bodies and for no other purpose. Therefore, the Society cannot be held liable for any act made or document issued by other parties on the basis of the statements or information given by the Society. The validity, application, meaning and interpretation of a Certificate of Classification, or any other document or information issued by the Society in connection with its Services, is governed by the Rules of the Society, which is the sole subject entitled to make such interpretation. Any disagreement on technical matters between the Interested Party and the Surveyor in the carrying out of his functions shall be raised in writing as soon as possible with the Society, which will settle any divergence of opinion or dispute.

3.3. The classification of a Ship, or the issuance of a certificate or other document connected with classification or certificati on and in general with the performance of Services by the Society shall have the validity conferred upon it by the Rules of the Society at the time of the assignment of class or issuance of the certificate; in no case shall it amount to a statement or warranty of seaw orthiness,

structural integrity, quality or fitness for a particular purpose or service of any Ship, structur e, material, equipment or machinery inspected or tested by the Society.

3.4. Any document issued by the Society in relation to its activities reflects the condition of the Ship or the subject of certifi cation or other activity at the time of the check.

3.5. The Rules, surveys and activities performed by the Society, reports, certificates and other documents issued by the Society are in no way intended to replace the duties and responsibilities of other parties such as Governments, designers, ship builders, manufacturers, repairers, suppliers, contractors or sub-contractors, Owners, operators, charterers, underwriters, sellers or intended buyers of a Ship or other product or system surveyed.

These documents and activities do not relieve such parties from any fulfilment, warranty, responsibility, duty or obligation (also of a contractual nature) expressed or implied or in any case incumbent on them, nor do they confer on such parties any right, claim or cause of action against the Society. With particular regard to the duties of the ship Owner, the Services undertaken by the Society do not relieve the Owner of his duty to ensure proper maintenance of the Ship and ensure seaworthiness at all times. Likewise, t he Rules, surveys performed, reports, certificates and other documents issued by the Society are intended neither to guarantee the buyers of the Ship, its components or any other surveyed or certified item, nor to relieve the seller of the duties arising out of the law or the contract, regarding the quality, commercial value or characteristics of the item which is the subject of transaction.

In no case, therefore, shall the Society assume the obligations incumbent upon the above-mentioned parties, even when it is consulted in connection with matters not covered by its Rules or other documents.

In consideration of the above, the Interested Party undertakes to relieve and hold harmless the Society from any third party claim, as well as from any liability in relation to the latter concerning the Services rendered.

Insofar as they are not expressly provided for in these General Conditions, the duties and responsibilities of the Owner and Interested Parties with respect to the services rendered by the Society are described in the Rules applicable to the specific Service rendered.

Article 4

4.1. Any request for the Society's Services shall be submitted in writing and signed by or on behalf of the Interested Party. Such a request will be considered irrevocable as soon as received by the Society and shall entail acceptance by the applicant of all relevant requirements of the Rules, including these General Conditions. Upon acceptance of the written request by the Society, a contract between the Society and the Interested Party is entered into, which is regulated by the present General Conditions.

4.2. In consideration of the Services rendered by the Society, the Interested Party and the person requesting the service shall be jointly liable for the payment of the relevant fees, even if the service is not concluded for any cause not pertaining to the Society. In the latter case, the Society shall not be held liable for non-fulfilment or partial fulfilment of the Services requested. In the event of late payment, interest at the legal current rate increased by 1.5% may be demanded.

4.3. The contract for the classification of a Ship or for other Services may be terminated and any certificates revoked at the request of one of the parties, subject to at least 30 days' notice to be given in writing. Failure to pay, even in part, the fees due for Services carried out by the Society will entitle the Society to immediately terminate the contract and suspend the Services.

For every termination of the contract, the fees for the activities performed until the time of the termination shall be owed to the Society as well as the expenses incurred in view of activities already programmed; this is without prejudice to the right to compensation due to the Society as a consequence of the termination.

With particular reference to Ship classification and certification, unless decided otherwise by the Society, termination of the contract implies that the assignment of class to a Ship is withheld or, if already assigned, that it is suspended or withdrawn; any st atutory certificates issued by the Society will be withdrawn in those cases where provided for by agreements between the Society and the flag State.

Article 5

5.1. In providing the Services, as well as other correlated information or advice, the Society, its Surveyors, servants or agents operate with due diligence for the proper execution of the activity. However, considering the nature of the activities performed (see art. 2.4), it is not possible to guarantee absolute accuracy, correctness and completeness of any information or advice supplied. Express and implied warranties are specifically disclaimed.

Therefore, except as provided for in paragraph 5.2 below, and also in the case of activities carried out by delegation of Governments, neither the Society nor any of its Surveyors will be liable for any loss, damage or expense of whatever nature sustained by any person, in tort or in contract, derived from carrying out the Services.

5.2. Notwithstanding the provisions in paragraph 5.1 above, should any user of the Society's Services prove that he has suffered a loss or damage due to any negligent act or omission of the Society, its Surveyors, servants or agents, then the Society will pay compensation to such person for his proved loss, up to, but not exceeding, five times the amount of the fees charged for the specific services, information or opinions from which the loss or damage derives or, if no fee has been charged, a maximum of AED5,000 (Arab Emirates Dirhams Five Thousand only). Where the fees charged are related to a number of Services, the amount of the fees will be apportioned for the purpose of the calculation of the maximum compensation, by reference to the estimated time involved in the performance of the Service from which the damage or loss derives. Any liability for indirect or consequential loss, damage or expense is specifically excluded. In any case, irrespective of the amount of the fees charged, the maximum damages payable by the Society will not be more than AED5,000,000 (Arab Emirates Dirhams Five Millions only). Payment of compensation under this paragraph will not entail any admission of responsibility and/or liability by the Society and will be made without prejudice to the disclaimer clause contained in paragraph 5.1 above.

5.3. Any claim for loss or damage of whatever nature by virtue of the provisions set forth herein shall be made to the Society in writing, within the shorter of the following periods: (i) THREE (3) MONTHS from the date on which the Services were performed, or (ii) THREE (3) MONTHS from the date on which the damage was discovered. Failure to comply with the above deadline will constitute an absolute bar to the pursuit of such a claim against the Society.

Article 6

6.1. These General Conditions shall be governed by and construed in accordance with United Arab Emirates (UAE) law, and any dispute arising from or in connection with the Rules or with the Services of the Society, including any issues concerning responsibility, liability or limitations of liability of the Society, shall be determined in accordance with UAE law. The courts of the Dubai International Financial Centre (DIFC) shall have exclusive jurisdiction in relation to any claim or dispute which may arise out of or in connection with the Rules or with the Services of the Society.

6.2. However,

(i) In cases where neither the claim nor any counterclaim exceeds the sum of AED300,000 (Arab Emirates Dirhams Three Hundred Thousand) the dispute shall be referred to the jurisdiction of the DIFC Small Claims Tribunal; and

(ii) for disputes concerning non-payment of the fees and/or expenses due to the Society for services, the Society shall have the

right to submit any claim to the jurisdiction of the Courts of the place where the registered or operating office of the Interested Party or of the applicant who requested the Service is located.

In the case of actions taken against the Society by a third party before a public Court, the Society shall also have the right to summon the Interested Party or the subject who requested the Service before that Court, in order to be relieved and held harmless according to art. 3.5 above.

Article 7

7.1. All plans, specifications, documents and information provided by, issued by, or made known to the Society, in connection with the performance of its Services, will be treated as confidential and will not be made available to any other party other than the Owner without authorisation of the Interested Party, except as provided for or required by any applicable international, European or domestic legislation, Charter or other IACS resolutions, or order from a competent authority. Information about the status and validity of class and statutory certificates, including transfers, changes, suspensions, withdrawals of class, recommendations/conditions of class, operating conditions or restrictions issued against classed ships and other related information, as may be required, may be published on the website or released by other means, without the prior consent of the Interested Party.

Information about the status and validity of other certificates and statements may also be published on the website or released by other means, without the prior consent of the Interested Party.

7.2. Notwithstanding the general duty of confidentiality owed by the Society to its clients in clause 7.1 above, the Society's clients hereby accept that the Society may participate in the IACS Early Warning System which requires each Classification Society to provide other involved Classification Societies with relevant technical information on serious hull structural and engineering systems failures, as defined in the IACS Early Warning System (but not including any drawings relating to the ship which may be the specific property of another party), to enable such useful information to be shared and used to facilitate the proper working of the IACS Early Warning System. The Society will provide its clients with written details of such information sent to the involved Classification Societies.

7.3. In the event of transfer of class, addition of a second class or withdrawal from a double/dual class, the Interested Party undertakes to provide or to permit the Society to provide the other Classification Society with all building plans and drawings, certificates, documents and information relevant to the classed unit, including its history file, as the other Classification Society may require for the purpose of classification in compliance with the applicable legislation and relative IACS Procedure. It is the Owner's duty to ensure that, whenever required, the consent of the builder is obtained with regard to the provision of plans and drawings to the new Society, either by way of appropriate stipulation in the building contract or by other agreement.

In the event that the ownership of the ship, product or system subject to certification is transferred to a new subject, the latter shall have the right to access all pertinent drawings, specifications, documents or information issued by the Society or which has come to the knowledge of the Society while carrying out its Services, even if related to a period prior to transfer of ownership.

Article 8

8.1. Should any part of these General Conditions be declared invalid, this will not affect the validity of the remaining provisions.

INDEX

1 SCOPE

This Guide provides:

- an overview on Cyber threats,
- an overview on the actions to be put in place to maintain the security of the on board cyber systems
- a tool for assessing the work done by ship owners and operators on the minimization and management of -Cyber Security Risks.

2 REFERENCE TO OTHER REGULATIONS AND STANDARDS

Regarding in particular Cyber threats and actions to be put in place to maintain the security of the on board cyber systems, reference is made to the IMO document MSC 96/4/1 dated 4 February 2016 “The Guidelines On Cybersecurity On Board Of Ships” submitted at the 96th Session of IMO Maritime Safety Committee by ICS, IUMI, BIMCO, INTERTANKO, CLIA and INTERCARGO and IMO MSC-FAL.1/Circ.3 “Guidelines on Maritime Cyber Risk Management”.

3 APPLICATION

3.1 Ship and Off-Shore Units

This Guide applies to ship and offshore unit cyber systems which may be affected by cyber-attacks.

3.2 Company

They also apply to relevant shipowner and operator Companies ashore cyber system, and in particular to personnel who is to be involved at all levels in the management of the related risks.

4 DEFINITIONS

Unless otherwise stated, the terms used in this Guide has the definitions laid down in the IEC standards and ISO ISO/IEC 27000:2016.

The following definitions also apply.

- Access control is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.
- Alarm system is a system intended to give a signal in the event of abnormal running condition.
- Control system is a system by which an intentional action is exerted on an apparatus to attain given purposes.
- Critical systems are, as far as this guide are concerned, those systems that, when disrupted or functionally impaired, pose unacceptable risks to company assets.
- Cyber-attack is any type of offensive manoeuvre that targets cyber systems, computer networks, and/or personal computer devices attempting to compromise, destroy or access company and ship systems and data.
- Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In particular, on board ship and offshore units, it protects the operational technology against the unintended consequences of a cyber incident, the information and communication systems including the information contained therein against damage, unauthorized use or modification, or exploitation and/or against interception when data and information are transferred by means of communication systems and/or the internet.
- Cyber system is a system involving, using, or relating to computers; it is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services; examples include business systems, control systems and access control systems.
- Cyber risk is any risk related to to the failure of a cyber system.
- Cyber risk management is the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.
- Cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals or the environment through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (Adapted from "Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems" by NIST of United States of America).
- Denial of Service (DoS) is a form of cyber-attack which prevents legitimate and authorized users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack involves a cyber-attacker taking control of multiple computers and/or servers to deliver a denial of service attack.
- Firewall is a logical or physical break designed to prevent unauthorized access to IT infrastructure and information.
- Information security is the security applied to information (rather than systems) protecting it from unauthorized access, disclosure, modification or destruction.
- Malware is a generic term for a variety of malicious software which can infect computer systems and impact on their performance.
- Operational technology (OT) is a wording used to identify devices, sensors, software and

associated networking that monitor and control on board systems.
- Removable media is a collective term for all methods of storing and transferring data between computers; this includes laptops, USB memory sticks, CDs, DVDs and diskettes.
- Risk assessment is the process which collects information and assigns values to risks for setting priorities, developing or comparing courses of action, and informing decision making.
- Risk management is the process of identifying, analysing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.
- Software is the program, procedures and associated documentation pertaining to the operation of the computer system.

5 Overview on Cyber threats

The need to carefully consider cyber security matters is the consequence of the essential and critical importance assumed by on board cyber systems, data transfer between ship or offshore unit and shore, protection of digital information and data sensitive for the Company and related not only to the ship or offshore unit equipment or performance but also to the crew, the cargo and the passengers.

For an overview on Cyber threats, reference is made to the IMO document MSC 96/4/1 dated 4 February 2016 “The Guidelines on cybersecurity on board of ships” in particular in articles “Introduction” and “Understanding the cyber threat”.

6 Actions to maintain security of the Cyber Systems

Due to the importance of this issue, cyber security is to be a strategic responsibility of the Company’s top management and is to be the basis of an awareness path customized for all the personnel on board and on shore having access to the ship and shore network.

The NIST (National Institute of Standards and Technology – US Dept. of Commerce) has developed a framework to help Companies in identifying and prioritizing necessary activities to achieve specific cyber security outcomes.

The activities, organized in five "Functions"- Identify, Protect, Detect, Respond and Recover, are described in the IMO document MSC 96/4/1 dated 4 February 2016 “The Guidelines on cybersecurity on board of ships” in particular in Annex 1 NIST framework and in the IMO MSC-FAL.1/Circ.3 “Guidelines on Maritime Cyber Risk Management”.

7 RECOMMENDATIONS

7.1 General

The cyber security policy adopted and implemented by a Company has to focus on the systems involving a particular ship or offshore unit and the relevant on shore part of the cyber system.

7.2 Cyber Security Policy

7.2.1

The Company has to establish a cyber security policy.

7.2.2

The cyber security policy has to identify as a minimum:
- the need of involvement of all personnel at all level of the organisation
- the authority and the responsibility of the personnel involved in the management of the Company’s cyber security system
- the acceptable level of cyber risk (e.g. among low, moderate, high)
- the targets for which the cyber risks and the relevant end effects are to be identified and, as far as practicable, minimized to be kept at, or under, the acceptable level; this means that the risk is to be evaluated in terms of likelihood and consequence on crew personnel and passenger safety (see Note 1), ship propulsion and ship safety systems availability, environmental impact, cargo conservation and cargo handling system availability (see Note 1), passenger service availability (see Note 1), data loss and protection, data availability, communication availability, time to repair, reputation and so on
- the need of implementing appropriate (with reference to the identified risk) actions to recognize cyber system weakness and vulnerability, to be protected from unauthorized access, to detect abnormal network operation and cyber related incidents, preparedness to respond to and recover after a possible cyber incident or attack
- the procedure for the periodical review of the implemented actions, incidents and cyber system in view of continuous improvement of the cyber security
- the most appropriate training plan to increase the cyber risk awareness and related necessary knowledge at all company levels.

7.2.3

The cyber security policy is to be implemented on board and in the relevant on shore cyber system.

7.3 Cyber System Documentation

7.3.1

Documents are to be available to familiarize with the cyber system architecture.

7.3.2

They have to show any possible physical accessibility of the cyber system from outside, including ports for any removable equipment connection (from removable storage memories to computer, from wireless connections to internet or other communication and data transfer means).

7.4 Critical equipment and systems

7.4.1

Ship systems affected by possible malfunction of the cyber system are to be identified.

7.4.2

When their operation depends on the ship or ship shore cyber system, special consideration is to be given to systems such as:

- Propulsion and Fuel Oil System
- Steering system
- Main source of electrical power
- Alarm Systems
- Control Systems
- Safety Systems
- ESD (Emergency Shut Down) system
- Emergency source of electrical power
- UPS (Uninterruptable Power Supplies)
- Internal and external communication systems
- Fire extinguishing systems
- Safety center control system (for passenger ships)
- Bilge and ballast systems
- Heeling pumps
- Valves control and monitoring
- Power-operated watertight and semi-watertight doors (for passenger ships)
- Fire doors (for passenger ships)
- Flooding detection system (for passenger ships)
- Sanitation
- Grey Water system
- Specific Hotel services (for passenger ships) e.g. Laundry, Galley
- Refrigeration of food
- Lighting
- Ventilation and air conditioning
- Lifts (for passenger ships)
- Any other system whose disruption or functional impairing may pose risks at ship operation (e.g. LNG monitoring and control system, relevant gas detection system etc.)

7.5 Cyber Risk Assessment

7.5.1

A cyber risk assessment is to be carried out. It is to be conducted internally or by a third party, with the attendance of Tasneef.

7.5.2

The assessment has to cover as a minimum:

- identification of physical accessibility
- evaluation of the protection in place to ensure safe information exchange and safe data transfer between Ship/Shore
- implemented policies for the on-board software
- implemented policies regarding Password Management System and Account Management
- implemented back-up management policies
- tracking of critical events
- tracking of software, hardware and network modifications and management of changes
- examining the level of segregation of on-board architectures (automation and navigation networks, communications systems, network hosts and networking) and the criticality of potential contact points.

7.6 Identification

7.6.1

The cyber risk assessment is to include actions such as identification of personnel roles and responsibilities for cyber risk management and identification of the systems, assets, data and capabilities that, when disrupted or functionally impaired, pose risks to ship operations.

7.7 Protection

7.7.1

The cyber risk assessment is to include necessary actions for the evaluation of the protective measures already in place.

7.7.2

Depending on the assessment results, additional protective measures on the already implemented risk control processes and contingency plans to protect against a cyber-event and ensure continuity of shipping operations may be required.

7.8 Detection

7.8.1

The cyber risk assessment is to include necessary actions to identify the existing detection capabilities.

7.8.2

Depending on the assessment results, additional detective measures such as the development and implementation of activities necessary to detect a cyber-event in a timely manner may be required.

7.9 Response

7.9.1

The cyber risk assessment is to include actions such as the evaluation of the response capabilities.

7.9.2

Depending on the assessment results, additional activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event may be required.

7.10 Recovery

7.10.1

The cyber risk assessment is to include actions such as the evaluation of the recover capabilities.

7.10.2

Depending on the assessment results, additional measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event may be required.

7.10.3

Practical tests are to be performed at planned regular intervals, consistently with safe operation of the ship and equipment involved, possibly in occasion of Tasneef initial or periodical audit.

7.10.4

Alternatively, documented evidence that the test has been carried out as planned is to be available.

8 Statement of conformity

8.1 General

8.1.1

Upon Company request, good result of an initial audit, (this good result includes the verification of the implementation of the additional measures as required by the cyber risk assessment outcome, if any), Tasneef will issue a document stating the conformity of the cyber security system, as implemented on board of a specific ship or offshore unit, to the recommendations given in this Guide.

8.1.2

Tasneef is to be promptly informed by the company in the case of any changes occurring related to aspects which could influence the capacity to continue meeting the requirements of these Guidelines, and reserves the right to perform additional audits if the changes communicated are considered particularly relevant as regards maintenance of compliance with the requirements of these Guidelines.

8.2 Validity

8.2.1

The statement validity will expire in one year, unless confirmed by a yearly follow-up audit.

8.2.2

The statement validity will be suspended in accordance with the “General contract conditions governing system, product and personnel certification” and also

- upon Company request or
- in case the Company does not allow the annual audits to be carried out when due
- in case the Company has not met the deadline established for corrective action communication
- as a consequence of a major non conformity not resolved within the time limit established or
- as a consequence of numerous observations affecting the proper functioning of the cyber risk management process not resolved within the time limit established or
- in case the Company has carried out major restructuring without informing Tasneef of these changes or
- in case the Company has made significant changes to the cyber system which have not been accepted by Tasneef or
- in case of any justified and serious complaints received by Tasneef are confirmed.

8.3 Suspension

Suspension is notified in writing, stating the conditions for reinstatement of validity the statement and the deadline by which these are to be fulfilled.

8.4 Reinstatement

8.4.1

In case of suspension, to reinstate the statement validity, an additional audit is to be carried out.

8.4.2

Reinstatement is dependent on verification that the shortcomings, which led to suspension, have been eliminated.