INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

Ref. T2-OSS/1.4

MSC.1/Circ.1376
3 December 2010

CONTINUITY OF SERVICE PLAN FOR THE LRIT SYSTEM

1 The Maritime Safety Committee (the Committee), at its eighty-eighth session (24 November to 3 December 2010), for the benefit of SOLAS Contracting Governments and, in particular, of those involved in the operation of components of the LRIT system, approved the Continuity of service plan for the LRIT system, as set out in the annex.

2 The Continuity of service plan for the LRIT system (the Plan) includes procedures to address both the temporary suspensions of operations or reduction of the service provided, as well as measures to be taken in the event of critical failure to ensure the continuous provision of LRIT information or to recover operations in the event of a serious disaster. The Plan also provides a formalized governance framework to address any issues that may require immediate decisions or actions in order to safeguard the system.

3 The Committee also agreed to keep the Plan under review and to amend it as and when the circumstances so warrant.

4 SOLAS Contracting Governments are invited to bring the present circular to the attention of those engaged in the operation of their LRIT Data Centres.

5 The United States, having agreed to provide the International LRIT Data Exchange on an interim basis, is invited to bring the present circular to the attention of those engaged in the operation of the International LRIT Data Exchange.

6 SOLAS Contracting Governments, LRIT Data Centres acting through SOLAS Contracting Government(s) which have established them, the International LRIT Data Exchange acting through the United States and the LRIT Coordinator are also invited to bring to the attention of the Committee, at the earliest opportunity, the results of the experience gained from the use of the Plan set out in the annex for consideration of any action to be taken.

7 This circular revokes MSC.1/Circ.1344 on Interim continuity of service plan for the LRIT system, for the period between MSC 87 and MSC 88, issued on 13 May 2010, and any reference to MSC.1/Circ.1344 should be read as reference to the present circular.

***

ANNEX
(English only)

CONTINUITY OF SERVICE PLAN FOR THE LRIT SYSTEM

1 Introduction

1.1 The Long-Range Identification and Tracking (LRIT) system, which provides for the global identification and tracking of ships, consists of the shipborne LRIT information transmitting equipment, the Communication Service Provider(s) (CSPs), the Application Service Provider(s) (ASPs), the LRIT Data Centre(s) (DCs), including any related Vessel Monitoring System(s) (VMSs), the LRIT Data Distribution Plan (DDP), and the International LRIT Data Exchange (IDE). For the LRIT system to operate efficiently, all components of the LRIT system need to work seamlessly together to ensure the end-to-end transmission of messages between DCs requesting and providing LRIT information.

1.2 The provisions of SOLAS regulation V/19-1, the Revised performance standards and functional requirements for the long-range identification and tracking of ships (the Revised performance standards), and the Technical specifications for the LRIT system include a number of performance expectations of system components and thus of the LRIT system as a whole.

1.3 LRIT information is provided to SOLAS Contracting Governments and search and rescue (SAR) services entitled to receive the information, upon request, through a system of National, Regional, Cooperative and International DCs, applying applicable elements from the DDP provided by the DDP server and using the IDE to route all messages between DCs. Individual DCs, the DDP server and the IDE, are key interdependent system components that need to be continuously maintained in order to meet the expectations of SOLAS Contracting Governments and SAR services to receive prompt and reliable LRIT information.

1.4 While DCs, the IDE and the DDP server have been designed to ensure that SOLAS Contracting Governments and SAR services are provided in a timely manner the LRIT information they are entitled to receive upon request or as a result of standing orders, it is recognized that from time to time these system components may need temporarily to suspend their operations or to reduce the level of service provided in order to carry out, *inter alia*, scheduled or unscheduled maintenance or upgrade of hardware or software in use, or to manage or control unforeseen events such as malicious network attacks or deal with external reasons such as unavailability of, or access to, telecommunication networks, or to the internet or to conduct emergency or urgent repairs or maintenance which cannot be deferred to a later time.

1.5 The procedures for the notification, reporting and recording of temporary suspensions of operations of, or reduction of the service provided by, components of the LRIT system (the procedures for temporary suspension of operations or reduction of the service provided) set out in annex 2 to the annex to MSC.1/Circ.1294/Rev.2, provide procedures to be followed by DCs, the IDE and the DDP server when providing salient information to other components of the LRIT system and the LRIT Coordinator in cases where they have to temporarily suspend operations or reduce the level of service provided in cases of scheduled or planned activities and unforeseen events. These procedures also set out the records to be kept in such circumstances and their availability.

1.6 The procedures for temporary suspension of operations, or reduction of the service provided, are the first steps in building a more comprehensive Continuity of service plan for the LRIT system (the Continuity of service plan). Continuity management is the process by which plans are put in place and managed to ensure that information technology systems, such as LRIT, can recover and resume normal operations after a temporary suspension of operations or a reduction of the service provided, as well as in the event of a serious disaster. It is not just about reactive measures, but also about preventive measures – reducing the risk of downtimes and disaster in the first instance.

1.7 The LRIT system presents particular challenges as it is an interdependent and international system. The IDE, the DDP server and all DC operators must work collaboratively to ensure the continuing smooth operation of the LRIT system on a day-to-day basis, which in the event of a disaster or other unforeseen event may necessitate making major operational decisions within a very short time frame. A Continuity of service plan provides the globally agreed framework within which those decisions should be taken.

1.8 Incident management, which is primarily concerned with resolving the situation and getting the system back up and running, is only one element of a Continuity of service plan. The Continuity of service plan must also address problem management, which focuses on determining the root cause of an event and interfaces with change management to ensure that the problem is not a recurrent event.

1.9 A change management plan for matters related to the LRIT system is therefore an important component of the Continuity of service plan. One of the critical issues that needs to be agreed relates to the concept of a Change Control Board and overall ongoing governance of the LRIT system. This plan addresses elements to be considered in such a Board without presuming to prescribe its composition.

2 Temporary suspension versus disaster recovery

2.1 Interruptions to the continuity of service of the LRIT system could occur as a result of either a planned or unplanned temporary suspension or reduction of the service provided of any system component, as well as a more full-scale disaster resulting in a critical failure that necessitates a comprehensive disaster recovery plan and corresponding procedures.

2.2 The Continuity of service plan contains processes and procedures to address both the more routine temporary suspension, as well as measures to be taken in the event of critical failure. While such a plan must look at the system as a whole, given that there are three types of major system component in the LRIT system: the IDE, the DDP server and the individual DCs, it should outline measures to be taken in the event of, firstly, a temporary suspension or reduction of the service provided of each of these individual components; and, secondly, a disaster that results in a critical failure of each component.

Impact assessment: IDE

2.3 The IDE is a message handling service that facilitates the exchange of LRIT information amongst DCs to enable LRIT Data Users to obtain the LRIT information they are entitled to receive. The IDE routes LRIT information between DCs using the information provided in the DDP. Any suspension of operations or reduction of the service provided by the IDE has direct and immediate implications across the entire LRIT system. A critical failure of the IDE without a comprehensive disaster recovery plan would effectively shut down the LRIT system. There is therefore a requirement for the IDE operator to make significant and real time operational decisions 24 hours a day, 365 days a year.

Impact assessment: DDP

2.4 The DDP provides operational rules facilitating the exchange of LRIT information between DCs. Unlike the IDE, a transient failure of the DDP server to provide notifications and downloads of the DDP would not necessarily completely prevent the LRIT system from continuing to function, as messages can continue to be exchanged between DCs via the IDE, disabling the DDP version number checking function.

2.5 However, the unavailability of the DDP server could affect in particular DCs or the IDE, depending on the timing and requirements of those components for obtaining the latest versions of the DDP, potentially having serious ramifications on the normal operation of the LRIT system as a whole.

2.6 Furthermore, for compliance with the provisions of SOLAS regulation V/19-1, the availability of the DDP server should be regarded as a priority equal to that of the IDE, in order to ensure that the system is operating in accordance with the predetermined rules at all times.

Impact assessment: DC

2.7 The Revised performance standards stipulate that all DCs should establish and continuously maintain systems which ensure, at all times, that LRIT Data Users are only provided with the LRIT information they are entitled to receive as specified in SOLAS regulation V/19-1. In order to meet these requirements, DCs should have procedures and processes in place to address planned or unplanned interruptions to their systems. If a DC is not functioning, or is functioning at reduced capacity, the impact is felt by every other component of the system that relies on that DC to provide timely LRIT information. There is, therefore, an expectation that DCs have a 24-hour point of contact, identified in the DDP, in the event of an impediment to continuity of service.

3 Temporary suspensions of operations or reduction of the service provided

Notifications between components of the LRIT system

3.1 All notifications between components of the LRIT system should be performed using the contact details provided in the latest available version of the DDP.

3.2 The IDE should provide the necessary functionality in the IDE administrative interface to perform all notifications and publish and update advisory notices.

3.3 Access to the IDE administrative interface should be provided to the designated points of contacts for LRIT-related matters and the LRIT Coordinator, as listed in the DDP.

3.4 Whenever a new advisory notice is published, updated or removed, the IDE should automatically advise all designated points of contact for LRIT-related matters and the LRIT Coordinator.

Scheduled or planned activities requiring temporary suspension of operations or reduction of the level of service

3.5 System components requiring temporary suspension of operations or reduction of the level of service due to scheduled or planned activities should:

.1 publish an advisory notice on the IDE Administrative Interface at least five (5) days prior to the temporary suspension of operations or reduction of the level of service;

.2 confirm the advisory notice no later than 24 hours prior to the scheduled activity;

.3 remove the advisory notice after resuming normal operation; and

.4 complete a report on temporary suspension of operations or reduction of level of service available on the IDE Administrative interface no later than thirty (30) days after the occurrence.

3.6 The advisory notice should include information on the planned or scheduled activities to be conducted; indicate the dates and times between which the activities would take place; supply information on the consequences of the activities (for example, the IDE would not be available to provide services or the DDP server would be operating at a reduced rate); and advise, if possible, any measures or arrangements which the other components of the LRIT system may need to have to put in place in order to ensure the speedy and efficient resumption of normal operations or to manage any adverse effects.

3.7 Figure 1 illustrates the steps to be taken when a suspension of operations or reduction of level of service due to scheduled or planned activities occurs:

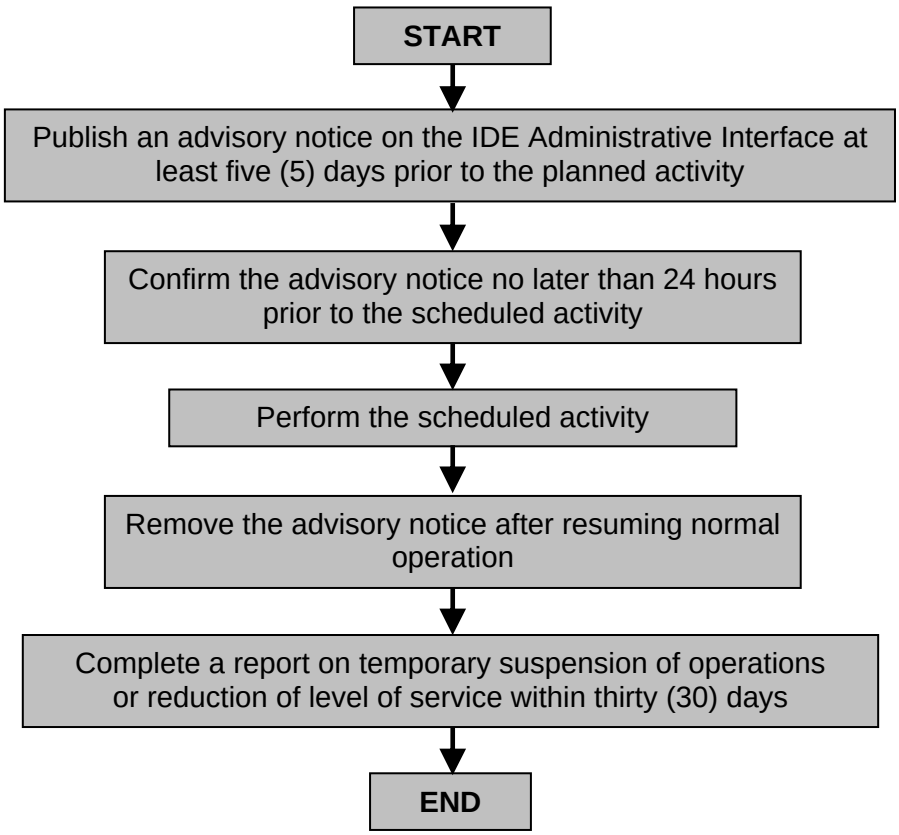

Figure 1 – Planned downtime notification flowchart

Unforeseen events requiring temporary suspension of operations or reduction of the level of service

3.8 Having identified an issue, the DC concerned, the IDE or the DDP server, as the case may be, should work collaboratively to resolve the issue. This may include contacting other components of the LRIT system using the contact details of the designated points of contact provided in the DDP.

3.9 Upon recognition or notification of an unforeseen event requiring temporary suspension of operations or reduction of the level of service, the system component concerned, the IDE or the DDP server, as the case may be, should try to resolve the issue and stabilize the component and, in particular:

.1 publish an advisory notice on the IDE Administrative Interface providing relevant information and including the expected time for resuming normal operation. Such a notice should be updated as and when developments occur;

.2 if, after 24 hours, the issue cannot be resolved, advise the LRIT Operational governance body[1], identifying the issue along with the measures or actions to be taken;

.3 once the system component concerned resumes or restores normal operation, remove the advisory notice from the IDE Administrative Interface; and

.4 complete a report on temporary suspension of operations or reduction of level of service available on the IDE Administrative interface no later than thirty (30) days after the occurrence.

3.10 If the issue is identified by the IDE or the DDP server, then the system component concerned should be contacted to resolve the issue. If the system component concerned cannot be contacted within 24 hours, then the IDE or the DDP server, as the case may be, should publish an advisory notice on the IDE Administrative Interface on behalf of the system component concerned.

3.11 Figure 2 illustrates the steps to be taken when a suspension of operations or reduction of level of service due to unforeseen events occurs:

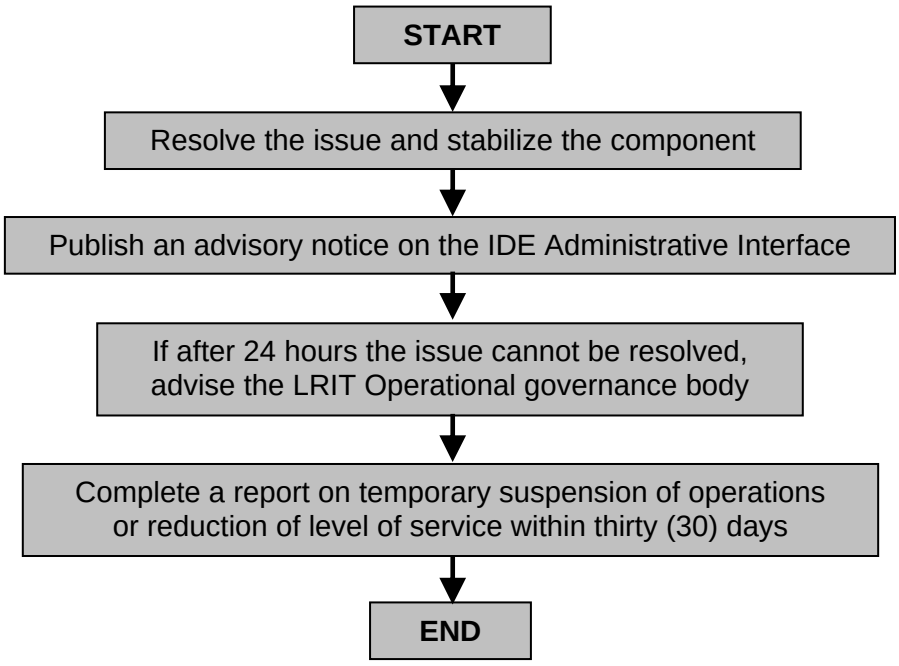

Figure 2 – Unforeseen events notification flowchart

[1] Refer to the Appendix – Governance of the LRIT system.

Identification of degradation in the level of LRIT service

3.12 If the IDE, the DDP server or a DC operator encounter degradation in the level of LRIT service as the result of issues believed to be the result of another component of the LRIT system, then the following actions should be taken:

.1 review known issues posted on the IDE Administrative interface to determine if the issue encountered was already identified by another system component;

.2 if required, use the tools available on the IDE Administrative interface to assist in troubleshooting the issue. This, for example, may include checking the IDE journal for routeing of LRIT messages or other networking functions;

.3 if the issue identified was the result of another LRIT system component, then the system component concerned should be contacted using the contact information available in the DDP; and

.4 if the system component is unable to resolve the issue after directly contacting the system component associated with the problem, or if the system component is unsure of the origins of the issue, and if the issue has reduced the operational capability of the system or is causing the LRIT system to not perform as designed, then the system component should follow the procedures specified in paragraphs 3.8 to 3.10 above.

Routine problems

3.13 In accordance with the Technical specifications for communications within the LRIT system, DCs and the DDP server, as the case may be, should transmit *System status* messages to the IDE every 30 minutes. These are being transmitted in order to provide the IDE with information pertaining to the operational status of the system component concerned.

3.14 If the IDE does not receive eight (8) consecutive *System status* messages from a specific DC and there has been no scheduled or unscheduled notification or advisory notice posted on the IDE Administrative interface by the DC concerned, then the IDE operator should post an advisory notice to the IDE Administrative interface and follow the procedures specified in paragraph 3.12 above. Upon notification, the DC concerned should follow the procedures specified in paragraph 3.9 above.

Issues related to the DDP version number checking function

3.15 In accordance with the Technical specifications for the International LRIT Data Exchange, the IDE should have the functional capability to validate the DDP version number contained in all received LRIT messages against the version number of the latest available version of the DDP.

3.16 The IDE operator is authorized to disable the DDP version checking function under circumstances that may cause or have caused a significant number of DCs and their associated SOLAS Contracting Government(s) to not be in conformance with the latest available version of the DDP and implemented by the IDE.

3.17 After disabling the DDP version number checking function, the IDE operator should follow the procedures specified in paragraph 3.12 above.

3.18 Once the issue is resolved, the IDE should enable the DDP version number checking function and advise all system components in accordance.

Invalid DDP upload (malicious or inadvertent)

3.19 Cases where the DDP file provided by the DDP server is invalid or cannot be properly processed may be separated into two categories:

.1 DDP content improperly formed (i.e. inverted polygons or other data contained within the DDP, where the DDP remains valid as per the XML schema); and

.2 a DDP file which is corrupted or otherwise invalid with regard to the XML schema.

3.20 In addition to the DDP processing procedures specified in sections 2.3.2 and 2.3.2A of the Technical specifications for communications within the LRIT system and in paragraph 3.12 above, the DDP server operator, after being notified of an issue, should take the following actions:

.1 analyse the reported problem and verify the issue. If required, the DDP server operator should request the IDE to disable the DDP version number checking function;

.2 advise all DCs, the IDE and the LRIT Coordinator about the issue;

.3 take all necessary actions to return all affected DDP versions to a valid state, including contacting the designated national points of contact for LRIT-related matters of the SOLAS Contracting Government(s) concerned, or removing or modifying data associated with the problem;

.4 contact the IDE and confirm that the issue has been resolved; and

.5 restore normal operation and notify all DCs, the IDE and the LRIT Coordinator, specifying any necessary actions to be observed or executed.

3.21 The Secretariat should report accordingly to the Maritime Safety Committee about any issue(s) with the DDP, as well as, any subsequent action(s).

PKI certificate compromise

3.22 The Organization, acting as PKI Certificate Authority (CA), issues PKI certificates for the testing and production environments of the LRIT system for use by DCs, the IDE and the DDP server in relation to communications within the LRIT system.

3.23 If a system component identifies an issue which may compromise the security of a PKI certificate, then the CA, after being notified of an issue, should take the following actions:

.1 as soon as a breach in security related to an issued PKI certificate(s) is discovered, the CA should notify the IDE and the DDP server operators. The IDE and DDP server operators should take immediate action to disable all communications using the compromised PKI certificate(s);

.2 revoke, in due course, the compromised PKI certificate(s) and publish an updated Certificate Revocation List. If necessary, the CA should contact the person in charge of the affected component for further information on the issue. The affected system component may submit a request for the issue of a new PKI certificate to the CA in accordance with the procedures issued by the Organization; and

.3 issue a new PKI certificate(s) for the affected system component to resume normal operation.

3.24 Any notification about PKI compromise should be originated from the person in charge of the DC, the IDE or the DDP server, as the case may be, or from a designated national point of contact for LRIT-related matters of a SOLAS Contracting Government.

3.25 The system component affected should also follow the procedures specified in paragraph 3.9 above.

3.26 The Secretariat should report accordingly to the Maritime Safety Committee about any issue with PKI certificates, as well as, any subsequent action(s).

PKI Changeover procedures

3.27 The following procedures should be observed during the PKI changeover:

.1 all PKI certificates should expire on the same date;

.2 the CA should be available before, during and after the time of changeover;

.3 the PKI changeover date should be, at minimum, two (2) weeks prior to expiration of the PKI certificates;

.4 new PKI certificates should be distributed at least two (2) weeks prior to the changeover date; and

.5 requests for the issue of PKI certificates should be submitted no less than six (6) weeks prior to the PKI changeover date.

4 LRIT Disaster Recovery

4.1 IDE Disaster Recovery

Critical failure circumstances

4.1.1 A critical failure circumstance could take place if the IDE sustains a critical failure (e.g., sustained power outage, sustained network connectivity degradation, etc.) at its host site and is not able to be reconstituted on hardware at the local host site and therefore must failover to hardware at the IDE Disaster Recovery (DR) site.

4.1.2 It is expected that an IDE DR capability would be provided for the IDE by either the primary IDE Operator or another entity.

IDE DR planning considerations

4.1.3 In accordance with the Technical specifications for the LRIT system, the IDE should have a DR site accessible every day of the year 24 hours a day.

4.1.4 The IDE DR site should have:

.1 full operational functionality;

.2 off-site storage of both full and incremental backups, including backups of the journal; and

.3 data and PKI synchronization at a minimum every 6 hours with the production environment of the LRIT system. The IDE should only be offline for a maximum period of 4 hours. With the synchronization set to 6 hours, there is a realized risk of a maximum loss of up to ten hours of journal information for the IDE.

4.1.5 The IDE operator should be cognizant of firewall restrictions at the DR site and should ensure there are no restrictions at the DR site on the IP addresses accessing the production system.

4.1.6 To institute a failover to the DR site, a Domain Name Server (DNS) change is required. Most systems should be set up to refresh within 15 minutes automatically. The DNS record for the IDE should be set up to expire and refresh every 10 minutes. However, if this switch does not automatically happen, then some systems components may need to be rebooted to institute the change. Upon refresh or reboot all systems components should be operational.

4.1.7 While the IDE is failing over to the IDE DR site, the DDP version number checking function should be disabled until the IDE operator determines that the system is stable.

IDE DR testing plan

4.1.8 The IDE DR should be tested once a year in the production environment and as determined by the IDE operator. The IDE should follow the notification procedures identified in the Procedures for temporary suspension of operations and reduction of level of service. The switchover of the IDE DR in production should be communicated in advance to the LRIT Operational governance body[2]. Critical success factors for the planned test should also be communicated via the notification process.

IDE DR management considerations

4.1.9 The IDE should be switched to the IDE DR site if the IDE operator estimates the downtime to fix an unplanned outage could take more than two (2) hours. The changeover can take up to two (2) hours. This provides for up to four (4) hours of service unavailability in the event of a critical failure of the IDE at its primary site, before which normal service should be resumed through the IDE DR site.

Notification process

4.1.10 Upon activation of the IDE DR process, the IDE operator should advise all DCs, the DDP server and the LRIT Coordinator that the IDE DR will be activated. If for any reason the IDE cannot perform the communication, then the IDE operator should contact the DDP server operator and request to perform the communication.

4.1.11 If the DDP server operator notes that three (3) or more *System status* messages from the IDE have been missed and there has been no scheduled or unscheduled notification or advisory notice posted on the IDE Administrative interface, then the DDP server operator should attempt to contact the IDE operator to determine the nature of problem. If, within 30 minutes, the DDP server operator is unable to contact the IDE, then the DDP server should advise all DCs and the LRIT Coordinator that there is a problem with the IDE and that the process for a failover to the IDE DR site could be activated.

[2] Refer to the Appendix – Governance of the LRIT system.

4.1.12 Once the IDE DR site is activated, the IDE should advise all DCs, the DDP server and the LRIT Coordinator indicating that the IDE DR operation is ready and commencing, the IDE DR plan is now in place and the instructions previously agreed upon and documented should be implemented.

4.1.13 The IDE should remain at the IDE DR site as long as necessary and until the IDE operator determines that the primary site is ready for a return to normal operations. As soon as the primary location is ready, the IDE operator should advise all DCs, the DDP server and the LRIT Coordinator at least 24 hours prior to the return to the primary location.

4.1.14 Upon recovery to the primary location, the IDE operator should complete a report as required in the procedures for temporary suspension of operations and reduction of level of service.

IDE DR dependencies

4.1.15 Full 24/7 support and operation of the DDP server to allow endpoint for PKI to be updated and for supporting the notification process, if necessary.

4.1.16 Synchronization with the production environment of the LRIT system (data, PKI certificates).

4.2 DDP server Disaster Recovery

Critical failure circumstances

4.2.1 A critical failure circumstance could take place if the DDP server sustains a critical failure preventing it from normal operation within the LRIT system, (e.g., sustained power outage, sustained network connectivity degradation, etc.), at its host site and is not able to be reconstituted on hardware at the local host site and therefore must failover to hardware at the DDP server DR site.

4.2.2 It is expected that a DR capability, including a 24-hour monitoring of the operational system for issue resolution and the handling of DDP server DR failover, will be provided by the Organization.

DDP server DR site planning considerations

4.2.3 In accordance with the Technical specifications for the LRIT system, the DDP server should have a DR site accessible every day of the year 24 hours a day.

4.2.4 During an unplanned outage, the DDP server operator shall have up to two (2) hours to resolve the issue and restore DDP server functionality. If the outage is estimated from the outset to require more than two (2) hours to resolve, or if after two (2) hours the service cannot be restored, the transitioning process to the DDP server DR site should be initiated. The transition process may take up to two (2) hours to be completed. This provides for up to four (4) hours of service unavailability in the event of a critical failure of the DDP server at its primary site, before which normal service should be resumed through the DDP server DR site.

DR infrastructure considerations

4.2.5 The DDP server system hosted at the DR site should have full operational functionality, providing all services as on the primary site during normal operation. The DDP server DR site should be maintained on an ongoing basis and be kept synchronized with the DDP server system at the primary site, in order to facilitate an emergency failover at any time.

4.2.6 In order to keep technical complexities within reasonable limits, the DDP server DR site may lag up to six (6) hours behind the DDP server at the primary site during normal operation. As a consequence, up to six (6) hours of system data may be irrecoverably lost should the DR plan be activated.

4.2.7 The transition to the DDP server DR site during a failover exercise should be as seamless as possible to minimize the impact on the LRIT system. The DNS entry of the DDP server should be set up to expire and refresh every 10 minutes to reflect its IP address at the DDP server DR site. This approach avoids the need to change the DDP server's web service URI and therefore the requirement for having a separate PKI certificate for the DDP server DR site. The IP address of the DDP server DR site should be communicated well in advance to all LRIT system components to enable firewalls and other routing devices to permit normal communications with the DDP server at its DR location.

4.2.8 The DDP server should participate in, and execute, planned DR failover tests of the LRIT system together with all other components, in accordance with the procedures adopted for such testing.

4.2.9 It is noted that the DDP server is implemented as a module of the GISIS system, and all provisions for the DR, and downtime related to the DR testing, would apply to the GISIS system as a whole, including the accessibility of all modules by Member States and members of the public.

Notification process

4.2.10 Upon activation of the DDP server DR process, the DDP server operator should advise all DCs, the IDE and the LRIT Coordinator that the DDP server DR will be activated. If for any reason the DDP server cannot perform the communication, then the DDP server operator should contact the IDE operator and request to perform the communication. If required, the DDP server operator should request the IDE to disable the DDP version number checking function.

4.2.11 If the IDE operator notes that three (3) or more *System status* messages from the DDP server have been missed and there has been no scheduled or unscheduled notification or advisory notice posted on the IDE Administrative interface, then the IDE operator should attempt to contact the DDP server operator to determine the nature of problem. If, within 30 minutes, the IDE operator is unable to contact the DDP server, then the IDE should advise all DCs and the LRIT Coordinator that there is a problem with the DDP server and that the process for a failover to the DDP server DR site could be activated.

4.2.12 Once the DDP server DR site is activated, the DDP server operator should advise all DCs, the IDE and the LRIT Coordinator indicating that the DDP server DR operation is ready and commencing, the DDP server DR plan is now in place and the instructions previously agreed upon and documented should be implemented.

4.2.13 The DDP server operator should also contact the IDE and confirm that the DDP version numbers are in sequence. If after the re-establishment of service at the DDP server DR site, the DDP versions of the IDE and/or DCs are no longer synchronized with the latest DDP version published by the DDP server, then the DDP server operator should take the necessary action to publish a new version of the DDP at an appropriate version number to ensure all components are able to retrieve and consistently apply the new version of the DDP. During this time the DDP version number checking should remain disabled until all DCs and the IDE can implement the current/new version of the DDP.

4.2.14 The DDP server should remain at the DDP server DR site as long as necessary and until the DDP server operator determines that the primary site is ready for a return to normal operations. As soon as the primary location is ready, the DDP server operator should advise all DCs, the IDE and the LRIT Coordinator at least 24 hours prior to the return to the primary location.

4.2.15 Upon recovery to the primary location, the DDP server operator should complete a report as required in the procedures for temporary suspension of operations and reduction of level of service.

DDP server DR dependencies

4.2.16 Full 24/7 support and operation of the IDE for supporting the notification process, if necessary.

4.2.17 Synchronization with the production environment of the LRIT system (data, PKI certificates).

Appendix

Governance of the LRIT system

1 The LRIT system, as an international operational system, requires a formalized governance structure. There have been and will be issues surrounding the operation of the LRIT system which have and will require immediate decisions or actions in order to safeguard the system. There are numerous issues that the system could face, from when to disconnect a DC from the IDE, to how to test the modification testing of new schemas, to whether a new message or function should be added to the system, and so on. Some of these issues would require immediate action, others more analysis, and still others a high-level management decision.

2 To address these varying types of issues, four different governance levels are required:

.1 Immediate decision: The various components of the LRIT system are being continuously monitored by their individual operators. Under specific circumstances, these operators must be required to make immediate decisions in order to resolve the issue and stabilize the component concerned.

.2 Operational governance: After the immediate decision has been made, and if the system cannot be returned by the operators to normal operation within 24 hours, then an LRIT Operational governance body must be engaged to make the decision as to the best way to proceed.

.3 Change control: The architecture, design, and operation of the LRIT system is defined by the Technical specifications for the LRIT system and under the framework of SOLAS regulation V/19-1 and the Revised performance standards. There must be a governance framework in place to ensure that the Technical specifications for the LRIT system can be modified where necessary, and in an effective and efficient manner.

.4 Management: There must be a body that has the final approval on all LRIT-related matters. Any relevant issue must be reported periodically to this body, which would have to consider the issue and decide the most appropriate action(s).

3 These four governance levels are currently defined within the LRIT system as follows:

.1 Immediate decisions: The IDE, the DDP server and DCs operators.

.2 Operational governance: The Committee, at its eighty-sixth session, decided to continue the arrangements that had been put in place by MSC 85, namely:

"*… in case the system faced an emergency situation or a malicious attack, those which faced or encountered such situations first, in consultation with the chairman of the Ad Hoc LRIT Group; the United States acting on behalf of the IDE; and the Secretariat acting on behalf of the Organization for matters relating to the DDP and the PKI should determine the actions to be taken so as to best protect the system; contain the propagation of the problem(s) to other components of the system; ensure continuity of service; and restore normal operations.*"

The LRIT Operational governance body is defined as the chairman of the *Ad Hoc* LRIT Group, a representative of the IDE, and a representative from the Secretariat.

.3 Change control: SOLAS regulation V/19-1 and the Revised performance standards are within the purview of the Committee. The Technical specifications for the LRIT system can be amended and accepted, on a provisional basis and subject to consideration and adoption of the related amendment(s) by the Committee, either by correspondence or via a meeting of the *Ad Hoc* LRIT Group, as specified in the Procedures for the consideration of proposals for the amendment of the Technical specifications for the LRIT system, the XML schemas and the Test procedures and cases, set out in annex 3 to the annex to MSC.1/Circ.1294/Rev.2.

.4 Management: The Maritime Safety Committee is the management body for the entire LRIT system.

4 It is recommended that the above governance structure be maintained. This includes holding meetings of the *Ad Hoc* LRIT Group as required.

5 The composition of the LRIT Operational governance body could be reviewed in future. For the effective and efficient operation of this body, its membership needs to be relatively small, organization members are preferable to individual persons, and it must reach decisions by consensus. This body should always contain a representative from the IDE, since the IDE is a critical central component of the system, and a representative from the Secretariat. The requirement for other member(s) needs further discussion.

6 The LRIT Operational governance body also needs to meet periodically (potentially bi-weekly via teleconference, if necessary) to discuss the operation of the system and to ensure that all operational issues are being addressed.

7 The Change control process, and the overall management of the LRIT system by the Maritime Safety Committee, has been working well during the design and early stages of implementation and operation of the system. Thus, there is no compelling need to make any changes to these processes, as what has been put in place has ensured the continuous operation of the LRIT system in compliance with the provision of SOLAS regulation V/19-1, the Revised performance standards and the Technical specifications for the LRIT system.