**Government of India**
**Ministry of Railways**
**(Railway Board)**

**No.2006/C&IS/PRS/Audit/4/Pt.I** **Sept. 1 , 2010**

**The General Managers**
All Indian Railways & Production Units

**The Managing Director**
CRIS, Chanakyapuri, New Delhi.

**CAO/FOIS, CAO/IS & CAO/PTS**

**The Director,**
Centralised Training Institutes

Sub.: **Crisis Management Plan of Indian Railways.**
Ref.: Railway Board's letter of even number dated 17.8.2010.

Kindly refer to above-mentioned letter from Railway Board (copy enclosed for ready reference) wherein while enclosing copy of the Crisis Management Plan (consisting of 8 pages), a compliance report was asked for. In this connection, it is informed that the last page of the Plan enclosed with the letter inadvertently concerned with another subject. The correct set of Crisis Management Plan is now being sent again for information & necessary action and with a request to send the compliance report at the earliest.

The above report has also been uploaded on Indian Railway website www.indianrailways.gov.in under C&IS Directorate.

**Encl.: As above.**

**(Suyash Narain)**
Director ME(C&IS)

**Copy to : All Executive Directors/Railway Board** – for kind information and necessary action.

**Government of India**
**Ministry of Railways**
**(Railway Board)**

**No.2006/C&IS/PRS/Audit/4/Pt.I** **August 17, 2010**

**The General Managers**
All Indian Railways & Production Units

**The Managing Director**
CRIS, Chanakyapuri, New Delhi.

**CAO/FOIS, CAO/IS & CAO/PTS**

**The Director,**
Centralised Training Institutes

Sub.: **Crisis Management Plan of Indian Railways**

In a meeting held on 12.3.2010, the Department of Information Technology had advised all Union Ministries and State Governments to submit their respective Crisis Management Plans. Accordingly, Ministry of Railways have prepared a detailed Crisis Management Plan for Indian Railways, a copy of which is being enclosed for information and necessary action. This plan has the approval of competent authority and has also been advised to Secretary, Deptt. of IT, Government of India. The same is attached for information and necessary action. A compliance report in this respect may also be sent to this office.

The above report has also been uploaded on Indian Railway website www.indianrailways.gov.in under C&IS Directorate.

**Encl.: As above.**

**(Suyash Narain)**
Director ME(C&IS)

**Copy to : All Executive Directors/Railway Board** – for kind information and necessary action.

# CRISIS MANAGEMENT PLAN

Indian Railways is the largest organized transport service provider in the country both in passenger and Freight sectors. In absence of a competitor in a similar mode of transport at national level, it becomes mandatory that the mode of transport, involving 1.4 million employees, is available on a 24x7 basis for 17 million passengers and 30 million tonnes of freight traffic everyday. To facilitate a smooth service delivery mechanism, and also to internally enhance efficiency, Indian Railways have gone in for computerization right from late sixties beginning with batch mode data processing accounting applications.

Decision to computerize the business activities and processes of railways was taken in the mid eighties, beginning with focus on service delivery mechanism in ticketing system. At the same time it was also decided to keep the systems abreast with state of the art technology and take advantages of development in technology to improve service delivery mechanism.

Keeping in line with the above objective, the applications developed/being developed, especially during last decade have been highly technology and infrastructure dependant. Therefore, the system design have greater focus on their 24x7 continuity & availability since it is now physically impossible to backtrack to manual days under any circumstances. Hence there is criticality for having a robust crisis avoidance/management plan for running these applications.

## CRISIS MANAGEMENT PLAN

Crisis Management plan for Indian Railways covers the entire range of applications currently running. Under the general Crisis Management Plan, there is provision for specific plans depending on the nature of applications. As per status of application in 2010, these applications have been categorized in order to enforce specific crisis management plan.

**Table 1**

| Sl No | Type | Name (example) | Stakeholders | Criticality | Primacy |
|---|---|---|---|---|---|
| 1 | Batch-mode stand-alone | Old EDP centers | Railway – Accounts | Fixed hours | Derived |
| 2 | Batch-mode networked | New EDP centers | Railway – Accounts | Fixed hours | Derived |
| 3 | OLTP – LAN + WAN | New office applications | Railway – multi departments | Fixed hours | Derived |
| 4 | OLTP – WAN | PRS, UTS | Public, Railway | 24x7 | Core |
| 5 | OLTP – Real-time – Centralized computing | FOIS, CMS etc | Public, Railway | 24x7 | Core |
| 6 | OLTP – Real-time – Distributed computing | COA | Railway | 24x7 | Core |
| 7 | MIS etc | Websites | Public, Railway | 24x7 | Derived |

Normally OLTP applications can be further segregated to two types – first referring to sequential reporting at a particular terminal level, second referring to sequential reporting at location level. For analytical purposes this segregation has been incorporated between above two categories of OLTP as opposed to OLTP – Real-time.

The above table indicates the type of applications currently running on the IR. However with passage of time, and as per organization's plan, the first three types will get merged with larger OLTP applications as derived systems and may not have to be run on a 24x7 basis as done for stand alone systems.

Besides these applications, there are more than 40000 PCs which act as independent work units which are linked through the net for exchange of information, notes etc. Some of them are critical to functioning of an individual or to a small group.

**Types of Crisis & their Management**

Crisis in a broader terminology with reference to Information Technology refers to any kind disruption to an on going system. Therefore Crisis Management refers to proactive measures taken for avoidance of such incidences and a well thought out plan along with remedial measures to recover and restore the system with minimum disruption.

Advanced developments in technology make it possible to overcome any kind of disruption. However, there is a huge price tag attached to such technologies. Therefore it is essential to understand the criticality of systems and place appropriate mechanisms to overcome such situations.

Crisis is of three different kinds: - **Sudden failure or non-availability of a critical component in a system (technical snags), Non-availability of the system (due to calamities, natural or man-made) and Cyber intrusion/attacks.**

Each of these crises affects different types of applications in different ways. Crisis management plan accordingly requires steps to be taken to avoid such interruptions. However, it is the measure of performance indicator (normally uptime) which ultimately decides whether the crisis management plan is the desired one or not.

Any kind of batch mode applications normally requires a low level of uptime or a high uptime for specified period during a day. However, this defined uptime can be achieved by adopting manual intervention processes, which avoids a heavy investment on physical resources. For example, there can be proxy reporting to ensure collection of data for inputs. In the long run, these applications do not hold any significance once the entire organization is automated on an end to end basis. These batch-mode applications get transformed and get merged with the MIS.

Therefore, in the long run, the applications will be of three types for which Crisis Management Plan has to be defined:

- Process based primary data inputs with desired service outputs
- Derived systems on the basis of primary data applications
- Ancillary Data warehousing systems for planning & performance review

**Action under Crisis Management Plan for type of application**

Since each type of application has varying level of required uptime, Crisis Management Plan has to define the availability of main components accordingly. This plan is valid for the first two types of likely crisis, whereas for the third type pertaining to the Cyber attacks/intrusions, the plan has to be completely different.

Given below a table, which outlines the kind of outages that can be tolerated for universally defined uptime for specific types of applications

**Table 2**

| Sl No | Type | System | Network | Infrastructure | Terminal |
|---|---|---|---|---|---|
| 1 | Batch-mode stand-alone | Tolerate Outages | Not Applicable | Not Applicable with local UPS | Not Applicable |
| 2 | Batch-mode networked | Tolerate Outages | Tolerate Outages | Not Applicable with local UPS | Not Applicable with proxy reporting or common terminal access |
| 3 | OLTP – LAN + WAN | Outages below 10% | Outages below 5% | Not Applicable with local UPS | Not Applicable with proxy reporting or common terminal access |
| 4 | OLTP – WAN | No Outage with DR provision | No Outage with route diversity | Continuous power supply | Certain %age of spare terminal available at site |
| 5 | OLTP – Real-time – Centralized computing | No Outage with DR provision | No Outage with route & media diversity | Continuous power supply | 100% redundancy along with proxy reporting |
| 6 | OLTP – Real-time – Distributed computing | No Outage with DR provision | No Outage at computing power | Continuous power supply | 100% redundancy |
| 7 | MIS etc | Outages below 5% | Outage below 1% | Continuous power supply | Not Applicable with common terminal access |

To maintain the defined uptime and avoid outages, different types of measures are taken by different organizations. They vary from having redundancy at component level within a box, on line redundancy of components, off line redundancy of components, proxy reporting depending on the tolerance level of the applications. However, there is a common accepted principle for arriving at such decisions. They are mapped in the following table matching with kind of anticipated outages given in the previous table

**Table 3**

| Sl No | Type | System | Network | Infrastructure | Terminal |
|---|---|---|---|---|---|
| 1 | Batch-mode stand-alone | Comprehensive AMC for maintenance | Not Applicable | Comprehensive AMC for UPS maintenance | Not Applicable |
| 2 | Batch-mode networked | Comprehensive AMC with provision for preventive maintenance | Comprehensive AMC for maintenance | Comprehensive AMC for UPS maintenance | Provision for proxy reporting or common terminal access |
| 3 | OLTP – LAN + WAN | Comprehensive AMC for on-site working hour support with provision for preventive maintenance | MPLS based connectivity with spare data-com equipment for replacement at WAN level | Comprehensive AMC with provision for preventive maintenance | Provision for proxy reporting or common terminal access |
| 4 | OLTP – WAN | Component-wise redundancy in the servers, 24x7 call support AMC with spares available with the AMC entity.<br><br>DR site is mandatory but synchronous replication depends on the criticality of the transaction data. | Route/Media diversity at WAN level with Diversity for local lead at the tier 0/1 levels of the network. Spare data -com equipment at all sites of tier 0/1 levels.<br>Monitoring through NMS | Continuous power supply through alternate sources with automated switchover mode | Certain %age of spare terminal available at all reporting site along with AMC attended during working hours |
| 5 | OLTP – Real-time – Centralized computing | Component-wise redundancy in the servers, 24x7 on-site supports AMC with spares available with the AMC entity as well as at server site.<br><br>DR site is mandatory but synchronous replication depends on the criticality of the transaction data. | Route/Media diversity at WAN level with Diversity for local lead at the tier 0/1 levels of the network. Spare data -com equipment at all sites of tier 0/1 levels.<br>Monitoring through NMS | Continuous power supply through alternate sources with automated switchover mode | 100% on-line redundancy at each site. |
| 6 | OLTP – Real-time – Distributed computing | Component-wise redundancy in the servers, 24x7 on-site support AMC with spares available with the AMC entity as well as at server site.<br><br>DR site is mandatory but synchronous replication depends on the criticality of the transaction data. | Route/Media diversity at WAN level with Diversity for local lead at the tier all levels upto distributed computing level of the network. Spare data -com equipment at all sites of all levels of computing levels.<br>Monitoring through | Continuous power supply through alternate sources with automated switchover mode | 100% on-line redundancy at each site. |

| | | | | | |
|---|---|---|---|---|---|
| | | | NMS | | |
| 7 | MIS etc | Component-wise redundancy in the servers, 24x7 call support AMC with spares available with the AMC entity.<br><br>DR site is desirable with asynchronous replication. | MPLS based connectivity with spare data-com equipment for replacement at WAN level | Comprehensive AMC with provision for preventive maintenance | Certain %age of spare terminal available at all reporting site along with AMC attended during working hours |

The above table refers to measures to be taken to tackle crisis referring to critical component level failures and system collapse due to all possible reasons. However, the third type of crisis, which is very common now-a-days, i.e. cyber attacks/intrusions call for a different kind of action plan for each of the above defined categories of application/systems.

**Table 4**

| Sl No | Type | System | Network | Infrastructure | Terminal |
|---|---|---|---|---|---|
| 1 | Batch-mode stand-alone | Local terminal level firewall protection | Not Applicable | Not applicable | Not Applicable |
| 2 | Batch-mode networked | Local terminal level firewall protection | Not Applicable | Not applicable | Not Applicable |
| 3 | OLTP – LAN + WAN | Firewall protection with firewall between WAN & LAN | MPLS based connectivity with Firewall before core router at the end of WAN links | Not applicable | Local terminal level firewall protection |
| 4 | OLTP – WAN | Firewall protection with IDS & IPS between WAN & Server and Firewall between LAN & server | Network with dedicated channels having managed data-com equipment for remote access through NMS | Not applicable | Local terminals with dedicated LAN connection. Prevention of use of external disks |
| 5 | OLTP – Real-time – Centralized computing | Firewall protection with IDS & IPS between WAN & Server and Firewall between LAN & server | Network with dedicated channels having managed data-com equipment with necessary security compliant and also for remote access through NMS | Not applicable | Local terminals with dedicated LAN connection. Prevention of use of external disks |
| 6 | OLTP – Real-time – Distributed computing | Firewall protection with IDS & IPS between WAN & Server and Firewall between LAN & each computing server | Network with dedicated channels having managed data-com equipment with necessary security compliant and also | Not applicable | Local terminals with dedicated LAN connection. Prevention of use of external disks |

| | | | | | |
|---|---|---|---|---|---|
| | | | for remote access through NMS | | |
| 7 | MIS etc | Firewall protection with IDS & IPS between WAN & Server and Firewall between LAN & server | MPLS based connectivity with Firewall before core router at the end of WAN links | Not applicable | Local terminals with dedicated LAN connection. Prevention of use of external disks |

**Preventive Periodic checks at the system level to avoid crisis**

Issues discussed above are design related issues which are supposed to avoid any kind of crisis situation. However, failures still may occur either due to a combination of reasons or due to un-anticipated erratic behavior of a component. Therefore there has to be a pre-defined drill to ensure perfect health of the system.

Today, all the high end products are bundled with on line & automated background monitoring of health of these products. But in most cases, the redundant components, equipment placed online (for OLTP WAN & OLTP Real time systems) for automatic switch over to avoid momentary failure do escape such monitoring systems. Therefore, mandatory pro-active checks are defined for these systems. Under this plan the following failure preventive checks are to be carried out:

**Processing power (servers)**

Normally servers are placed in clusters to run the applications on a High Availability mode. Within each server there is redundant power supply points, network controller. Normally these redundant components are active in an online system and failure of any single component is visible through the console. However at server level, unless they are in a load balancing mode, the performance of the stand by server is tested once a week by shifting the application from the normal active server.

**Communication Link availability**

For the OLTP application the WAN links at both tiers 0 & 1 levels are designed with both route/media service providers diversity with last mile diversity for each link (at least at the tier 0 level). Though all the links are in active mode, toggling (high bit error rate compared to minimum threshold) is normally not noticed except for momentary alerts on the NMS. Therefore, once a day all the links are tested individually by disabling the alternate link.

**Contingency Plan for worst case Scenario**

Not withstanding a robust design & 24x7 monitoring, there may be a rare occasion when none of the alternate IT systems are available. With a massive public interface and the manual systems being dispensed with, this kind of a collapse presents a

nightmarish situation which can be termed as a worst disaster case. Therefore it is essential that there is a Crisis Management Plan for this kind of eventuality.

From stakeholders point, all the IT applications fall under two broad categories: one dealing with external customers (PRS, UTS, FOIS etc), second dealing with internal customers (CMS, COA, LMS etc)

**Table 5**

| Application | Additional level protection | First Level Alert | Field level Action | Manual Action |
|---|---|---|---|---|
| PRS | For Charting – Periodic updation at one more node out of 5 centers besides skeleton chart once in six hours during last 24 hours | PRS centers alerts all CCMs & Sr DCMs through automated system | Roadside centers take chart position from the Main centers for emergency use | Nil |
| | Ticketing – System resident Fare table available in hard copy with stations | PRS centers alerts all CCMs & Sr DCMs through automated system | Use of Card tickets at major stations & BPTs at the counter as per quota | Data entry into terminals for subsequent updation into system |
| UTS | Nil – Client terminals can work as stand alone system for 72 hours | NIL | NIL | NIL |
| FOIS | Replicated Transaction data to be taken out of DW system and downloaded to client terminal through zonal EMS for print out | Zonal EMS centers alert COMs, CCMs, Sr DOMs & Sr DCMs | Use of paper RRs | Data entry into terminals for subsequent updation into system |
| COA | Replication of last 24 hours transaction data at CAS | CAS alerts COMs & Sr DOMs | Manual controlling with print out of data from CAS | Data from automated arrival/departure system updates the COA servers |
| CMS | Client terminal to have provision for storing last 24 hours booking data only for emergency print out | Zonal EMS centers alert COMs, Sr DOMs & the control office alerts all filed level lobbies | Client terminal should be able to continue work with provision for storage for 24 hours | Client terminals update the system |
| All other applications | To follow one of the above models depending on nature of design for processing & transaction data storage | To follow one of the above models depending on nature of design for processing & transaction data storage | To follow one of the above models depending on nature of design for processing & transaction data storage | To follow one of the above models depending on nature of design for processing & transaction data storage |
| MIS | All transaction data transferred to DW system at least once in a day, besides the specific defined periodicity | | | |

## Abbreviations

OLTP – On Line Transaction Processing
WAN – Wide Area Network
LAN – Local Area Network
DR – Disaster Recovery
MIS – Management Information System
PRS – Passenger Reservation System
UTS – Unreserved Ticketing System
FOIS – Freight Operations Information System
NMS – Network Management System
EDP – Electronic Data Processing
AMC – Annual Maintenance Contract
UPS – Uninterrupted Power Supply
CMS – Crew Management System
COA – Control Office Application
LMS – Loco Management System
DW – Data Warehousing
EMS – Enterprise Management System
CAS – Central Application System
BPT – Blank Paper Ticket
RR – Railway Receipt
COM – Chief Operations Manager
CCM – Chief Commercial Manager
Sr DOM – Senior Divisional Operations Manager
Sr DCM – Senior Divisional Commercial Manager