Abstract—Current day business and industry environment demands an inbuilt disaster management plans and procedures as part and parcel of organizational design fabric. An effective disaster recovery methodology is an important aspect of networked institutions operating under an umbrella of Educational Societies/Trusts for their day-to-day operations. In this research a Dynamic Disaster Recovery Management Model has been proposed with the focus of ensuring business operations’ connectivity and network functionalities even under duress. This model caters for detailed planning, effective communication amongst quick reaction recovery teams and alternative means of communication, through the analysis of continuous network performance monitoring and the associated results. Thus this model enables us to minimize loss of information due to the ongoing disaster and earliest possible recovery of services to enhance the service levels of the user community.

Keywords—In built disaster management, Dynamic Disaster Recovery Management, Quick reaction recovery team

I. INTRODUCTION

Disaster is generally defined as an activity breakdown that causes a service interruption or discontinuation of an important component of a system, including information infrastructure, for an indefinite period of time [1]. We can call this, as an Operational interruption, defined as any event, that disrupts the normal course of functioning for an known time period.

Capability to restore the service of vital functions by implementing Disaster recovery plan (DRP), a document that defines the roles, responsibilities and a team of people to manage an effective recovery is essential for any organization. The DRM should address risk scenarios that could result in partial or total breakdown of process continuity and management systems and most importantly the network. Popular strategies to recover a system may include the following actions:

- Response to quickly locate and replace failed Components to restore the system’s to their functional state.
- Timely re-establishment of the operations of the over all system from damaged conditions.
- Bringing up all the workstations and servers to provide quick relief to the users.
- Quick access and updation of anti-virus vaccines and activating security systems like IDS/DOS and other attack resistant software components.

With the growing dependence on IT/Networks and the Business Processes to support operational growth and changes associated with their complexities, there is a need to consider the elements that are critical to implement Dynamic Disaster Recovery Program (Critical Application Assessment, Back-Up Procedures, Recovery Procedures, Implementation Procedures, Test Procedures, and Plan Maintenance). [2]

Risk analysis is the most important issue to have the clear understanding of DRP/DDRM for any institution. Table 1 lists some of the common IT failures that disrupt operations. The other risk types are grouped into various disaster categories. Nearly every organization in the world faces feasible risks from many if not all of them. [3]

<table>
<thead>
<tr>
<th>Table 1: Generic Disasters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Disaster</strong></td>
</tr>
<tr>
<td>Natural Disaster</td>
</tr>
<tr>
<td>Man Made/Disaster</td>
</tr>
</tbody>
</table>

© 2014, IJARCSSE All Rights Reserved
A. Negative Effects of Disaster Specific to Educational Institutions

Breakdown and loss of information for a short time, with long-lasting effects on Education & Training business and research that can contribute to the demise of the otherwise well performing institutions:

- Loss of revenue from the consultancy projects
- Diminished societal credibility and students, parents& Faculty trust, resulting in churn
- Penalties for violated SLAs with business partners, and co-developers.
- Costs of recovering and repairing the lost data
- Generic costs of meeting internal and external compliance requirements to meet the needs of accreditation agencies.

CEOs, COOs, IT Directors’ and Vice Chancellors should consider scenarios in which normal operations could be disrupted and adopt/ adapt practices and technologies that enable them to deal with potential disruptions from hostile, external actions as well as internal system failures and also the natural calamities.

II. Current Day Disaster Recovery Models & Practices

We analyze cost effective and optimally suited models to meet the requirements of networked institutions being practiced across the globe and there are plenty of variations to DRM mechanisms in the literature and some of them are listed for information and deeper understanding.

In his paper, Kelly [4] defines a clear model that is highly beneficial in the management of disasters because it facilitates explicitly and precisely and supports disaster management processes. He also suggests the need of a formal system, or a model, to manage and possibly reduce the negative effects of a disaster.

Kimberly [5] suggests a four phase model for disaster management. This model portrays response as the biggest and most visible phase of disaster management. It places mitigation and preparation at the base, suggesting that they are both driving forces behind a successful response. The recovery phase takes the largest amount of time and is costliest one. The limitation of this model is that it is very much focused on emergency management in hospitals and cannot be significantly used in other applications. Since this model is restricted to hospital emergency management, its scope is limited.

An open-ended process model developed by Tuscaloosa [6] also contains four phases with the cycle begin and end with mitigation and an on-going attempt to limit the effects of a disaster.

Manitoba-Health-Disaster-Management [7], model has altogether six independent elements such as a strategic plan, hazard assessment, risk management, mitigation, preparedness and monitoring and evaluation. Each element observes its own boundaries and involves its own set of activities and processes.

The advantage of this model is that it provides a balance between preparedness and flexibility in order to respond dynamically to the specific needs of disasters. Since this model provides the link between actions and events in disasters such links can be tightly coupled.

In his model, Weichsegartner [8] (assesses the possible damage and the planning of future actions to reduce this possible damage. Here it is important that all measures taken are constantly reviewed and assessed. The model illustrates the process cycle and the integration of geographical area-based concepts in disaster management.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure related disaster</td>
<td>Software Errors, System Break down, Data loss, Connectivity of Network, Links and and software failure</td>
</tr>
</tbody>
</table>

Fig.1. Disaster recovery management Practices
Based on our survey of relevant literature, we have separated different disaster management models into the following main categories: logical, integrated, cause and Generic. These disaster management models are, shown in Figure 1. Logical models provide a simple definition of disaster stages and emphasize the basic events and actions which constitute a disaster. Integrated models characterize the phases of a disaster by the evolution of functions such as strategies etc. The Cause models provide frameworks for understanding the causes of a disaster. The growth of vulnerability of an organization is revealed and the underlying causes that fail to satisfy the demands of the users are identified. The models then estimate the dynamic pressure and unsafe conditions. The Indian Ocean tsunami and its impact on millions of people in that region demonstrated the high degree of vulnerability of people in disaster situations despite the existing predisposing factors in place (Blaikie et al., [9]). The last category, describes miscellaneous models. In all these models, various modules are linked as events and actions and all are shown in the diagram given below.

In the literature there are some integrated disaster management models which are the means of organizing related activities to ensure their effective implementation. Five main components of such systems can be identified as Risk assessment, Risk management, Loss Minimization, Recovery Readiness and Testing & Utilization. The first task in an integrated disaster management model is Risk assessment which provides the information necessary for the next phase. These results in decision making about the balance of mitigation and preparedness actions needed to address the risks.

A. General issues in Disaster recovery management

It is well known fact that a large number of activities are involved in mitigating disasters and recovering services. It is the involvement of this large number of activities that raises the problem of complexity in Dynamic Disaster Management. We elaborate on the issues of complexity that evolve from the management of such activities and highlight the characteristics of a complex environment. The characteristics that make dynamic disaster management a more complex domain are as follows:

- Many number of activities involved with widely varying features and functionalities.
- Dynamically changing environmental conditions, during and after the disaster
- Really a global perspective dynamic decision support system can address the issues.
- More Data of the gets scattered at various plan from different sources
- System Complexity is unimaginable.
- The decision-making process to handle
- Lot of uncertainty and vague inspectors.

Very big volume of diverse data, and the characteristics of the dynamic disaster management domain (which can be viewed by analyzing the activities elaborated in Figure 2), makes it impracticable to develop an integrated dynamic disaster management system to cope with all these activities. There is a need for high-level of coordination and the flow of information is immense and such information must be communicated between various groups of the organizations and agencies in the event of a disaster. Hence, the need arises for an integrated communication platform.

In their work Mc Entire [10] and Auf der Heide [11] pinpoint that the ability to communicate, coordinate and work effectively as a team will be the deciding factor for the success of any emergency plan. In response to these issues, we highlight the main problems associated with the development of dynamic disaster management systems as listed below.

- Design and development of processes for dynamic monitoring of the entire institutional resources
- Laxity & Failure in maintaining communication links and computing systems.
- Low system performance to data that makes for delayed updating of disaster-indicative information
- Issues in dynamic disaster-related data collection, processing and integration and generating triggers.
- Effective Communication and collaboration among all participants
- Deploying the decision support system to help managers achieve effective decision-making for different disaster management activities such as mitigation, preparedness, response and relief
- The need of multiple models are required for decision-making
- Understanding & validating environmental affects which can significantly minimize the severity of a disaster. Thus the below mentioned figure depicts the critical components of the DDM domain.

Fig.2.Critical Components of the DDRM
III. THE PROPOSED DYNAMIC DISASTER RECOVERY MANAGEMENT

With the focus of providing a specific solution to our networked institutions we propose a Dynamic Disaster Recovery Management Model, with the key components as depicted in Fig.3. The characteristics and functionalities of each component are explained in the succeeding paragraphs.

A. Dynamic Disaster recovery Management Planning

The DR planning process is a multi-faceted constraint optimization problem. The objective is to minimize, the loss of resources, latency impact on application, and rupee cost of the solutions. That can enable quick operational readiness the constraints are the properties of the namely replication capabilities, CPU, Speed, network and reliability, storage Capacity, interoperability constraints for instantiating the solution within the available resources across implementing all sites [12]. Basic objectives of a DDRMP are to support and guide an organization in the event of a disaster and effectively reestablish critical business operations within the shortest possible period of time with minimal loss of information. The goals of the planning project are to assess current and anticipated vulnerabilities, define the requirements of the operational units.

1. The DDRP must cater for the following technical areas
   a. Computing systems issues
   System configuration (disk capacity, peripheral devices, device names, RAM, file systems and volume groups, OS users, etc.) and operating system version and updates planning process is to ensure that DDRP machines have at least as much capacity as the earlier systems that are being replaced, and are compatible in all respects.
   b. Connectivity & Network problems
   Total networking requirements and issues need to be identified, documented, and to be included in the DDRP. With the special focus on LAN/Wan and associated network components like switches/routers etc.
   c. Software related
   Software encompasses many things. Software includes the Operating System, applications, and third party software (RDBMS, report writers, GUI products, backup/recovery products, scheduling software, etc.). A comprehensive inventory of currently used software, including current version, license information, and support contact information is essential.

B. Institutional Risk Analysis

Here we mitigate unnecessary risk and The scope of this effort includes people, software, equipment, and infrastructure. Any way “big picture”, Must cover the following
- Failure impact and the failure probability
- Average occurrence of failure per year
- Expected yearly loss
- Tentative cost of DDRMP

Fig.3. Key components of Dynamic Disaster recovery management
C. Dynamic Disaster recovery management strategy
- Backup and recovery facilities activation at the central site of the institutions.
- Cloud based service Recovery for service resumption.
- Shifting of operations to the central site with backup.
- Immediate repair and replacement of failed systems.
- Activating of all VMs for updating. The traffic away from the failed network service by activating alternative means of communications.

D. Operational continuity plan
Operational continuity describes the processes and procedures an institution must put in place to ensure that mission-critical functions can continue during and after a disaster. Potential Operational continuity problems may include the illness or departure of key team members, supply chain breakdowns, catastrophic failures or critical malware infections. Operational continuity planning means formalizing a institutional strategy for dealing with the unexpected and unknown by planning, training and testing for the recovery of critical business processes and IT systems in a timely fashion to minimize the impact of any disruption on the business and the customer.

E. Disaster recovery response mechanisms
Now we analyze various recovery methods available for each entity and determine the best suitable recovery method for each. This includes the resources employed in recovery and the process of recovery. Some of the typical entities are data systems, power, data network, and telephone systems. for each of these there are one or more mechanisms in practice in the industry.

F. Disaster recovery Implements
The process of defining business continuity and disaster recovery strategies and responses helps us to determine respond if a potentially disruptive incident occurs. In a normal sequence of BC/DR planning activities, strategy and response definition occurs after the business impact analysis and risk assessment phases, and precedes the BC/DR plan development phase.

G. Functional action after Disaster recovery
The recovery phase’s disaster assessment function should be integrated with the emergency response phase’s emergency assessment function in identifying the physical impacts of the disaster. Short-term recovery focuses on the immediate tasks of securing the impact area.
H. Organizational continuity plan and Validation

Considering the shortcomings of currently available systems, methodologies and approaches for crisis management and disaster recovery, we propose our model for effective communication and collaboration among the entities/colleges and government agencies for operational continuity and rapid disaster recovery. DDRM aims at addressing the entire organizational setup and Emergency Operations Center needs. We analyzed the necessary information requirements for our educational society, where the colleges are located at four different sites. Our methodology focuses on alternative means of primary communications and network management.

- Communications within the colleges/Departments affected by a crisis/disaster
- Communications between the colleges affected by the crisis/disaster and the related agencies outside the disaster area.
- Communications between the college and the Emergency Operational Centre at the central site,
- Communications between the Emergency Operations Center, and other sites.
- Communications between the Emergency Operations Centers affected by the crisis/disaster and the all other relevant agencies both within and outside the crisis/disaster area

The model is designed to assist the aforementioned communications and supports intra-collegiate collaboration, intercollegiate collaboration, collaboration between the departments and the government agencies such as BBMP, BSNL and State government agencies. The model (Fig. 5) identifies the key information elements that assist business continuity and rapid disaster recovery. These elements are:

- **Mobile Communications Vehicles**: Communications within and between organizational colleges and Emergency Operations Centers within and outside crisis/disaster.
- **Local Damage Assessment**: Damage assessment conducted by college/departments and emergency management team.
- **Recovery Plan Execution**: Identification and execution of recovery plans

IV. DYNAMIC DISASTER RECOVERY MANAGEMENT SOLUTION

DDRM solutions normally fall short of satisfying Institutional requirements due to the following aspects

- High Cost of the mobile communication
- Complexity connectivity, interoperability and networking issues.
- Reduced reliability due to the complex and build situation created by the disaster.

The complexity was high because, of the recovery of entire operational services and the recovery plans had to manipulate many individual components and mobile elements: applications, hosts, network, and storage. Reduced reliability of these procedures was diminished by low automation and inability to test any recovery procedure under disaster conditions. Virtualization helps the complexity of hardware and software and allows standardization of processes, thus making planning and automation of the recovery procedures much more reliable and repeatable.

Dynamic disaster recovery management solution provides

- The simplest way to replicate applications to a secondary site
- The simplest way to set up recovery and migration plans and
- Fully automated, highly reliable site recovery and migration

A. Simple and Efficient DDRM

Simple and of virtualization and the evolution of replication technology, DDRM is becoming more cost-effective. Since virtualization enables infrastructure consolidation at the failover site. Less costly replication options are more broadly available, using lower-end storage appliances or stand-alone software solutions. This, DDRM protects large-scale mission-critical IT assets, as well as smaller sites and other applications recovery.
B. DDRM Automation

Customers are generally shielded from the complexity of managing each step in the recovery process, because of the automated DDRM solutions that execute and coordinate all the steps required to ensure the desired level of protection. Setting up a recovery plan in a virtual environment is as simple as selecting RPOs and RTOs for each college/department service.

C. Stable site recovery

With virtualization, Educational institutions get much stronger assurance to meet their RPOs and RTOs. Since Virtualization provides the ability to test recovery plans frequently in a non-disruptive manner. Manual recovery processes are now replaced with automated recovery, eliminating the risk associated with user errors and ensuring predictable recovery.

DDRM is a complex task requiring special skills and expensive resources.

D. Couple of the Key processes for simple DDRM

- Fault tolerant system design through the cost of fault tolerant system is slightly higher than the regular process and it is always advisable to procure and install at the disaster prone sites, specially the critical computing and communicating network devices.
- Quick action to switch over to a redundant or standby communication link, network server or upon the failure or termination of an existing asset. It should happen without human intervention.
- Failback is the process of restoring a system or another asset that is in a failover state back to its original state. Effective failback returns the system to the state of operation before the disruption.
- Though the metrics like RPO & RTO [14] are not very critical for all our institutions but are essential because of the day to day operations of some of the colleges/departments.

V. Dynamic Network Disaster Recovery Plan and Providing Alternate Network Communications

A resilient distributed network environment is essential for delivering standard and high availability along with operational continuity and disaster recovery. Business continuation allows users to access storage, services [15] and local or remote servers (physical or virtual) – irrespective of their location and dependency on the service provider.

A. Off-Site Backup Mechanism

We have a good back up process in our organization with continuous data protection and full file-level restoration, to offload the burden of installing, managing, monitoring as well as complete restoration after a disaster.

![Off-Site Backup Mechanism](image)

Our encrypted server files are sent to an onsite backup manager (Central site), which are then sent to a secondary, offsite backup manager, to reduce the chances of the secondary site being affected by the same disaster or interruption. We are also in the process of implementing cloud based backup produce to minimize the cost and affection use of technology and expertise.

B. Network Replication and resilience

With today technology, cloud-based disaster recovery allows to ship a copy of the virtual server image offsite to run on a cloud server in the event of a disaster. But, for our institution more complex server configurations, much more than just a server image is required for recovery. Firewall rules, VLANs, VPNs and the network replication need to be fully replicated at the site before the site because operational central.

In order to achieve rapid recovery time objectives (RTOs), the server and network must be fully replicated at the secondary site in synchronicity with the operational site as
C. Shared Recovery Sites:
In the standard one-to-one deployment, a single data center is protected by a single recovery site. We have chosen to protect multiple data centers of our colleges using a “shared” recovery site. All protected sites are visible and manageable within this single instance of the DR solution at the shared recovery site. This topology has been implemented using the shared recovery site features.

D. Stand by/Alternate communication system
Includes all the planned mobile terminals, ready to move to the disaster location at short notice as per the directions of the recovery team manager. During the normal conditions, these terminals will be effectively used for scaling up the operational services from the required site to another one to cater for the special requirements of that segment of users. Thus these resources work as reserves for operational need and as disaster teams for encountering any unexpected eventuality. Hence the investment is not an additional burden but an effective utilisation of the communication resources.

E. Testing
It is planned to test the DDRM every year for numerous reasons to verify the working state of the plan and training our team in the process. Testing helps to figure out the weaknesses, or gaps in the process that need to be addressed. According to NIST, the following areas should be tested:
• Notification procedures
• System recovery on secondary site
• Internal and external connectivity
• System performance with secondary equipment
• Restoration of normal operations
Testing with a traditional disaster recovery plan can be time consuming and costly due to the retrieval, restoration and system re-configuration required, and often conventional plans are rarely tested through a full failover scenario. With cloud based disaster recovery, testing is easier, faster and less disruptive to your production environment and business operations than traditional disaster recovery. Since the cloud offers offsite backup of the entire virtual server in sync with the Central site.

![Fig.9 Generalized static model of operational centers for disaster recovery](image)

**VI. CONCLUSION & FUTURE WORK**

Basic aim of Dynamic Disaster Recovery Management Model is to minimize information loss and also the reputation loss to ensure stability of the brand name of the institutions. Accessibility and availability for regular use and quick response and faster downloads of the content at critical junctures like conduct of exams, results declaration, grading, students’ admissions and also employee performance analysis. Further our model enables the effective care and maintenance /recovery of the infrastructure needed for the interaction of students, teachers, and management, parents, researchers, industry and government agencies and also the society in general for the overall growth and development of educational system itself. The proposed solution has been tested at a reduced scale with the resources of the alternate communication system, in order to ensure basic minimum investment for Dynamic Disaster Recovery Management. Hence this model is one of the cost effective solutions for any networked institution to be competent for sustaining business operations.

**REFERENCES**


