



Consultant Report CR/2

May 31, 2006

CDMP DMIC ICT Strategy

SSA 05-17049

UNOPS Project No. BGD/01/004

Prepared by:

Sidney Tupper
Consultant

UNITED NATIONS OFFICE FOR PROJECT SERVICES

Bangkok, Thailand

CDMP DMIC ICT Strategy

Table of Contents

1	Introduction	1-1
1.1	Project Background	1-1
1.2	Document Purpose.....	1-1
1.3	Strategy Definition Methodology	1-1
2	DMIC Terms of Reference	2-1
2.1	Objectives.....	2-1
2.2	Functions.....	2-2
2.3	Media.....	2-8
3	Strategies for Information Sharing.....	3-1
3.1	Barriers to effective information sharing.....	3-1
3.1.1	Technical	3-1
3.1.2	Institutional	3-2
3.1.3	Financial	3-2
3.2	Initiatives and Incentives to Develop Information Sharing Capacity.....	3-3
3.2.1	Technical	3-3
3.2.2	Institutional	3-3
3.2.3	Financial	3-4
3.3	Data Sharing Agreements.....	3-4
4	ICT Implementation.....	4-1
4.1	Incremental Development	4-1
4.1.1	Data acquisition	4-1
4.1.2	Information Generation.....	4-2
4.1.3	Information Dissemination	4-2
4.2	Training	4-3
4.3	System Architecture	4-3
4.4	Network Requirements.....	4-5
4.5	Implementation Costs.....	4-5
4.5.1	Equipment	4-5
4.5.2	Operations.....	4-6
4.5.3	Training.....	4-6
4.6	Design Considerations	4-7
4.7	Sustainability	4-8
4.7.1	Technical	4-8
4.7.2	Institutional	4-9
4.7.3	Financial	4-9
5	DMIC Management Plan	5-1
5.1	Operational Scenarios.....	5-1
5.1.1	Normal operation	5-1
5.1.2	Emergency operation	5-2
5.2	DMIC Staffing	5-3
5.2.1	Organization	5-3
5.2.2	Job descriptions.....	5-4

Appendices

- A Data sharing Memorandum of Understanding outline

CDMP DMIC ICT Strategy

Tables

Table 2-1 Rationale of DMIC Candidate Functions.....	2-3
Table 2-2 Administration Tools	2-8
Table 2-3 DMIC media	2-8
Table 3-1 Necessary data sharing partners	3-1
Table 4-1 DMIC user training	4-3
Table 4-2 DMIC equipment costs.....	4-5
Table 4-3 Estimated 3 year cost of services and consumables	4-6
Table 4-4 Estimated 3 year DMIC labour costs	4-6
Table 4-5 Training costs.....	4-7
Table 5-1 DMIC daily operational activities.....	5-1
Table 5-2 DMIC emergency activities	5-2

Figures

Figure 2-1 Comprehensive Disaster Management Model.....	2-1
Figure 4-1 A possible DMIC development schedule	4-1
Figure 4-2 Strawman DMIC hardware architecture.....	4-4
Figure 5-1 DMIC operations staff organization	5-3

CDMP DMIC ICT Strategy

Acronyms

BBS	Bangladesh Bureau of Statistics
BDT	unit of Bangladesh currency
BMD	Bangladesh Meteorological Department
BTTB	Bangladesh Telephone and Telegraph Board
BWDB	Bangladesh Water Development Board
CBT	Computer-Based Training
CDMP	Comprehensive Disaster Management Program
CDROM	Compact Disk Read-Only Memory
CEGIS	Center for Environmental and Geographic Information Services
CEO	Chief Executive Officer
CPP	Cyclone Preparedness Program
CR	Consultant Report
CRA	Community Risk Assessment
CRMIS	Central Relief Management Information System
DBA	DataBase Administrator
DC	Deputy Commissioner
DMB	Disaster Management Bureau
DMC	Disaster Management Committee
DMIC	Disaster Management Information Centre
DMIN	Disaster Management Information Network
DRR	Directorate of Relief and Rehabilitation
DRRO	District Relief and Rehabilitation Office
DVD	Digital Video Disk
EOC	Emergency Operations Centre
FFWC	Flood Forecasting and Warning Centre
GDACS	Glogal Disaster Alert and Coordination System
GIS	Geographic Information System
GPRS	General Packet Radio Service
GPS	geographical positioning system
GSM	Global System for Mobile communication
GoB	Government of Bangladesh
ICT	Information and Communication Technology
ISD	International Subscriber Dialing
IVR	Interactive Voice Response
MOU	Memorandum of Understanding
MS	Microsoft
MoA	Ministry of Agriculture
MoFDM	Ministry of Food and Disaster Management
NGO	Non-Government Organization
NWD	Nation-Wide Dialing
NWRD	National Water Resources Database
PIO	Project Implementation Officer
PMO	Prime Minister's Office
QA	Quality Assurance
RS	Remote Sensing
SMS	Short Messaging Service
SOD	Standing Orders on Disasters
SSA	Special Service Agreement
SoB	Survey of Bangladesh
T&T	Telephone and Telegraph
UNOPS	United Nations Office for Project Services

CDMP DMIC ICT Strategy

UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
WAP	Wireless Access Protocol

CDMP DMIC ICT Strategy

1 INTRODUCTION

1.1 Project Background

Bangladesh suffers from increasingly frequent and devastating natural calamities due to its environmental situation, population density and development stage. Cyclones, tornadoes, river erosion, floods, drought and other extreme natural and man-made events greatly hinder the development of the country with loss of lives, livelihoods, assets and infrastructure. Profound and widespread poverty exacerbates the population's vulnerability to catastrophic episodes.

The disaster management community has expressed a need for more effective and better coordinated information management systems, aimed to improve coordination among agencies at all levels with access to appropriate, timely and accurate information before, during and after emergency situations. The Emergency Operations Centre (EOC) of the Ministry of Food and Disaster Management (MoFDM) is the responsible agency but is ill-equipped and lacks adequately skilled professional staff to carry out its required functions. Without modern telecommunication networks and integrated management systems, the EOC depends on district and upazila authorities to report critical information for decision-making using traditional communication methods that delay response. Consequently the Ministry will replace the EOC with a Disaster Management Information Centre (DMIC) located on the sixth floor of the Disaster Management and Relief Bhaban in Mohakhali, Dhaka. It will be equipped with modern Information and Communication Technology (ICT) to acquire topical information and serve it to stakeholders during normal and emergency periods, for policy implementation, support of risk reduction activities and real-time emergency response.

1.2 Document Purpose

This document has the following purposes:

- provide a focus for discussion of an evolving DMIC terms of reference
- facilitate a common understanding of DMIC ICT strategy
- steer DMIC systems design and operations planning

1.3 Strategy Definition Methodology

The approach taken to establish a coherent strategy for using ICTs to implement the MoFDM's objectives for disaster management is consultative and sensitive to stakeholders' existing ICT capacities, with the following steps:

- Prepare a strawman strategy based on initial thinking about DMIC operations, consistent with the CDMP Framework
- Identify key MoFDM stakeholders for collaborative consultation
- Incorporate DMIC Needs Assessment findings
- Develop an iterative review process to refine the strategy according to stakeholder inputs
- Maintain the strategy to reflect current thinking about DMIC operations
- Adjust the strategy according to the success of implementing incremental DMIC phases.

CDMP DMIC ICT Strategy

2 DMIC TERMS OF REFERENCE

2.1 Objectives

DMIC Goal:

The DMIC will implement effective information sharing among disaster management agencies and communities, for all hazards, in all sectors, in normal times and emergencies, throughout the nation and regionally, to support sustainable risk reduction and emergency response capacity.

To achieve this goal, the DMIC will employ appropriate, available and sustainable information and communication technologies to ensure timely acquisition, processing and dissemination of accurate disaster management information. Accommodating the diversity of stakeholder capacities to provide and receive information requires corresponding DMIC flexibility to use a variety of communication media to implement the information flows indicated in the DMIC Needs Assessment Report.

The DMIC will further national disaster management objectives and support MoFDM leadership in the disaster management community by providing essential information that engages and motivates and aids users. It will link the Disaster Management Committee hierarchy with the Ministry electronically.

The DMIC will support CDMP components' objectives in the framework of the Comprehensive Disaster Management Model, shown in Figure 2-1.

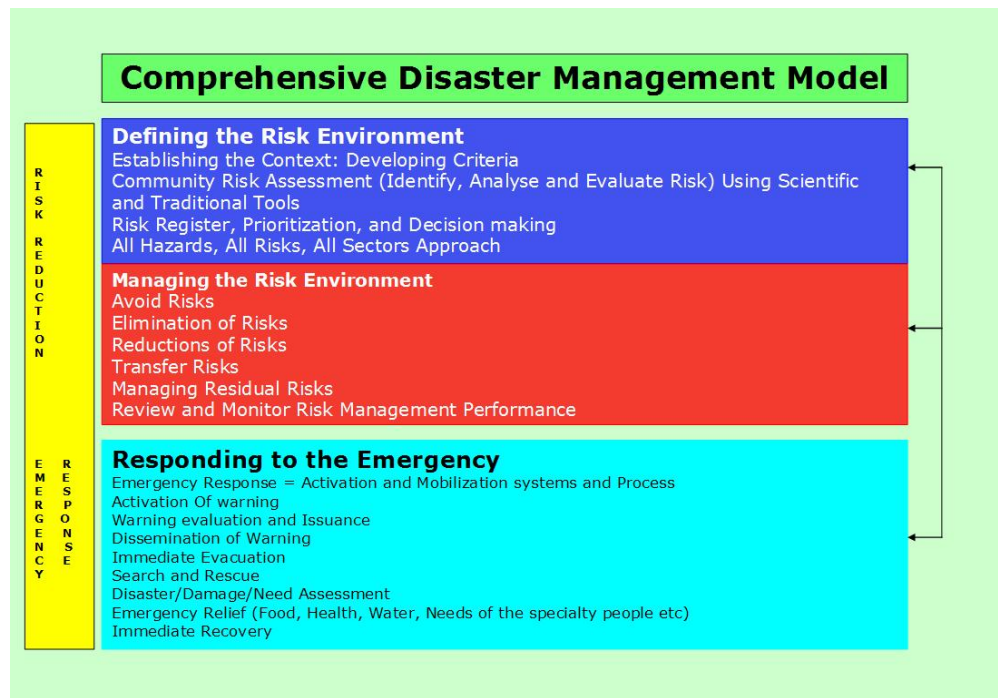


Figure 2-1 Comprehensive Disaster Management Model

CDMP DMIC ICT Strategy

2.2 Functions

In the current disaster management environment, BMD and FFWC adequately disseminate their early warning information to the district level, and through the CPP, cyclone alerts reach communities. Similarly the Prime Minister's Office gets situation intelligence directly from its sources during emergencies. Without adding value to their information the DMIC cannot significantly improve on this, and users might even see a transmission delay in information coming through the DMIC. To clearly justify itself as a valuable disaster management contributor, the DMIC must provide new services and benefit more stakeholders. It should provide functions that support the objectives of CDMP components. In normal times when no emergency exists, the DMIC should still provide attractive useful information and services to maintain stakeholders' motivation and familiarity, and to continuously exercise system functions. For example, the DMIC could display dynamic information that supports agricultural decisions, such as crop input costs, commodity prices, weather forecasts, inundation predictions and soil moisture observations, to users to visit the portal frequently.

Table 2-1 lists functions that have been suggested by and/or proposed to the primary stakeholders.

CDMP DMIC ICT Strategy

Table 2-1 Rationale of DMIC Candidate Functions

Mode	Phase	Function	Rationale
Risk Reduction	Normal times	Knowledge base of best practices for disaster management	Support awareness and improvement of institutional capacity for disaster management. The material would be uploaded by users and moderated by DMIC staff. Many projects' reports are in the public domain and could be usefully made available in the DMIC.
		Repository of disaster management literature	
		Project reports	
		Standing Orders on Disaster (SOD), directives and SOD-required outputs online	SOD is the principal policy and procedures document of the GoB for disaster management and should be widely available. Directives should be similarly available. Public availability of SOD-required outputs will improve transparency and accountability of GoB agencies in disaster management responsibilities.
		Historical hazard/disaster incidence and impacts database	Support research and understanding of hazards and their impacts
		Training resources: Computer-based training (CBT) modules, training material, lesson plans, trainers' contact information	Many agencies produce training material. Improve training quality by sharing the information; reduce redundant effort. CBT can improve training effectiveness and reduce costs.
Directory of disaster management institutional contacts	A subscriber-based directory of people and institutions would foster linkages, interaction and collaboration among members of the disaster management community.		

CDMP DMIC ICT Strategy

Mode	Phase	Function	Rationale
		Maintenance of information-sharing MOUs	MOUs define the information interfaces between sharing agencies. Changes must be reflected in the MOUs, which are the basis for common understanding and quality assurance.
		Information quality assurance	Information quality must be adequate to justify user confidence in the data; otherwise it will not be used. Tools and resources have to be applied to continuously assess quality, report problems and effect correction.
		CDMP component / GoB / NGO communication support	Disaster management agencies can use the DMIC to disseminate information by several media, interact in discussion forums and use collaborative tools. They can use DMIC media (web, WAP, SMS, IVR) to collect their field data into databases.
		Portal	A portal would gather in one place the user interfaces to many of the functions described in this table. Additional features including daily environmental and market information, news feeds, discussion forums, user-configured portal views and alert subscription tools would attract frequent use of the DMIC by internet users.
	Preparatory	Risk assessment tools and status	CRA methodology documentation, base data, field data entry tools and databases of CRA results will improve CRA productivity and encourage standards compliance for consistent practice and easier data sharing.

CDMP DMIC ICT Strategy

Mode	Phase	Function	Rationale
		Emergency response readiness plans and status	GoB agencies required by the SOD to maintain plans and prepare reports would make them available on DMIC for wide visibility to other agencies. The QA function could identify non-compliant institutions and encourage corrective action.
		Relief resources availability	Inventories of relief resources would reveal gaps for remedial action, and improve transparency and accountability. This would result in more effective and efficient application of relief resources.
		Institutional capacity status	Ongoing assessments of institutional capacity and publication of the results would identify gaps and encourage improvement. Informed understanding of NGOs' current capacities will result in more effective procurement of NGO services.
Emergency Response	Response	Hazard warnings	Although FFWC and BMD widely distribute their warning bulletins, some agencies receive warnings from only from the mass media, delayed and abbreviated. DMIC could send timely email/ SMS/ IVR alerts to subscribers according to their individual requirements, and post them on the portal.

CDMP DMIC ICT Strategy

Mode	Phase	Function	Rationale
		Loss (deaths, damage, etc.) reporting and analysis	Various agencies have implemented diverse manual systems for damage reporting, eg, the MoFDM's D-form and CPP damage reports, that accumulate and aggregate information upwards in their organizational hierarchies. The DMIC could provide an on-line system that reduces the timeliness and information-loss of the current systems and improves the usability of the data by standardizing its structure. Analyses would improve, based on more detailed, comprehensive and timely datasets.
		Relief needs (water, food, shelter, medical) and availability	Real-time supply and demand status of relief resources would enable timely identification of redundancies and gaps and more efficient, effective distribution.
		Emergency response coordination Internal DRR operations Multiple GoB agencies and NGOs International response: GDACS	Web-based GIS decision support tools and situation blogs which reflect the real-time resources, actions and intentions of the various autonomous emergency response actors would foster common situational understanding and an effective triage response, with less redundant effort and gaps. These tools encourage lateral accountability among actors and should serve inter-agency committees at several levels.
	Recovery	Resource need and availability Credit Public health Reconstruction materials	Real-time supply and demand status of recovery resources would enable timely identification of gaps and more efficient, effective distribution.

CDMP DMIC ICT Strategy

Mode	Phase	Function	Rationale
		CRMIS – DRR relief management system	Supporting the DRR recovery project management methodology with an information system will improve its effectiveness and reduce bureaucratic latency.
		recovery programs	A location-referenced catalog of recovery programs in implementation by the large and diverse development community would foster a common understanding of the national situation, eliminating redundant efforts and highlighting gaps.

CDMP DMIC ICT Strategy

Additionally the DMIC will include administration tools to manage the information it handles, the media it uses and the users it supports. Table 2-2 lists some of these.

Table 2-2 Administration Tools

Administration Tools	Purpose
Portal Framework	An application server which provides portal structure, user authentication and authorization, user preference management, flexible security policy and a variety of functions including <ul style="list-style-type: none"> • forums • event calendar • customer relations management tool • project management tools • database support • GIS tools • dissemination servers: email, fax, SMS and IVR
Content Management System	Enables standards-compliant maintenance of portal content by clerical staff with limited website creation skills, and displays content according to user preferences.
Mail/SMS/IVR list server	A database application that manages subscriptions of email, SMS and IVR users who receive information in those media.

2.3 Media

Analysis of commonalities among communication characteristics of the various hazard warnings reveals limited opportunities for employing one medium for several hazards. Their diverse natures in terms of message size, frequency and user capacity require in general that the choice of hazard warning medium varies with the hazard and audience that they address.

Assessment of DMIC user needs and information products indicates that the DMIC should support the media described in Table 2-3 to meet its information sharing objectives.

Table 2-3 DMIC media

Medium	Purpose
email	The DMIC should use email to send early warning information, bulletins and newsletters to subscribers of these services.
web	The DMIC portal should display information proposed in Table 2-1 and offer tools for decision support and emergency response coordination to users. It should provide an administrative interface for management of content, media and users.
SMS	The DMIC should implement an SMS gateway, message generation tools, subscriber lists to support generation and dissemination of SMS alerts for early warning, and data acquisition functions.
IVR	The DMIC should implement an IVR gateway, Bangla voice content tools and subscriber lists to support dissemination of alerts by voice.
couriers	The DMIC should courier information products that are too large to be disseminated by other media, or are aimed at users with no capacity to receive them by electronic means.

Early warning and emergency response communication media need to be exercised frequently to ensure availability in an emergency. Real emergencies are so infrequent that

CDMP DMIC ICT Strategy

the alarm infrastructure and user capacity are likely to deteriorate in the meantime, to the extent that the alarm fails and/or the users do not understand the information. Drills are effective but tend to dull user response due to the “cry wolf” syndrome. Routine use of the medium for some additional practical purpose valued by the users, such as daily weather reports, agricultural information and education, is best.

Emergency response communication media need to be redundant. A failure mode analysis should be conducted on each information flow to understand how to improve availability during hazard conditions when the communication infrastructure may be degraded.

Early warning media do not have to be so reliable or redundant as response media, since their use is likely to be prior to disruptions caused by the hazard condition. However, compound hazards need to be accommodated, in the sense that early warnings of more hazard events may have to be disseminated during an emergency. For example, during a flood emergency, warnings of water-borne diseases may be required.

CDMP DMIC ICT Strategy

3 Strategies for Information Sharing

3.1 Barriers to effective information sharing

Long-established custom and its inherent inertia may resist the introduction of new information sharing mechanisms. Even when implemented, information sharing is a difficult activity that requires near-constant attention to maintain useful performance on all sides of the institutional relationships. The following sections describe some of the technical, institutional and financial obstacles to be overcome.

3.1.1 Technical

Effective information sharing depends on timely availability of relevant, accurate and complete data. The present institutional environment has several technical shortcomings which stand in the way of achieving these qualities.

Bureaucratic process and information storage in Bangladesh are predominately paper-based and depend on the movement of physical file folders and letters among officials. Since just one official can be in possession of a file at a given time, no other official can take action affecting the file. Files can be corrupted or lost. When the file becomes inactive at the end of a project or fiscal period or whatever its scope may be, it is likely to be thrown away. Although a document in the file may have been prepared and printed with a computer, for retrieval purposes it exists only in the file. The retrieval and distribution of information in this form require the specific consent of the file holder and his action for photocopying and courier or postal delivery. This environment will persist until modern business practices enabled by ubiquitous computers, accessible databases and high-capacity networks replace the current practice at all levels and sectors of government. Inevitably this will happen, but not in the timeframe of CDMP.

Public administration staff lack necessary office automation skills. These will come as the Government provides the technology, but the scale of implementation and human resource development is huge and will take time.

Digital connectivity has greatly improved in the recent past with promise of further imminent progress. Few areas remain without GSM and GPRS mobile network coverage, which brings text messaging and narrow-band internet potential to almost everywhere in the country. However, GPRS is expensive in comparison with dial-up service, which could be provided economically by land line if BTTB's network coverage were increased. In practical terms, therefore, internet range is limited to districts and those upazilas with T&T service. To be a truly effective medium for disaster management, the internet needs to reach unions. Again, this is inevitable, but the timing is uncertain, and unlikely to be complete within the next several years.

Interoperability of systems in Bangla and English is immature and will always be problematical. A recently introduced Unicode Bangla character set still has issues that constrain its usefulness, such as poor support for sorting. Although numbers are easily transliterated between the two languages, dual-language database implementations significantly complicate text handling. Since for the foreseeable future English will be the technical lingua franca among national-level administrators and local-level governance will continue to be conducted in Bangla, information sharing will suffer from the need to translate between the two languages on flows up and down between the levels.

CDMP DMIC ICT Strategy

3.1.2 Institutional

Bangladesh institutions are unaccustomed and unmotivated to share information among themselves. They consider that giving away information can be giving away advantage. The cost to collect, analyze, organize, store and retrieve information is significant and not to be incurred gratuitously.

Archaic communication methods limit the capacity of the civil service to support the necessary competitiveness of Bangladesh industry in global markets, participate with international partners in development efforts to reduce poverty, meet the expectations of a growing population for good governance and specifically, respond effectively to mitigate the hazards endemic in this country. The present administrative environment has its origins in Mughal and British governance systems which were effective in their day. They managed a small fraction of today's population in an age when the acceptable time frame for information gathering, decisions and action was magnitudes longer than it is now. The formal hand-delivered letter is the traditional communication mode used in the civil service to traceably request, inform and direct. Delivered also in copies to other receivers for their use, it is also a testament to the fact that the message has been expressed, but it has the disadvantage of introducing a day of latency in transmission. Other disadvantages are that it is a hardcopy document with consequently awkward storage and retrieval and is difficult to forward or reuse. The days of dependence on formal hand-carried letters for propagation of control and inter-agency communication must be left behind.

Failure to effectively document and distribute procedures at the directorate level causes operational uncertainty when an officer encounters an unfamiliar situation, compels the chief executive to micro-manage and delays response. Well-established operational policies and procedures empower officers to make local decisions that need not be referred to higher authorities, for more timely and efficient response. They resist political influence for counter-productive action.

Other institutional weaknesses, which in general are beyond the capacity of CDMP and the Ministry to remedy but nevertheless significantly constrain the achievement of their goals, need to be understood. Placing more importance on performance rather than just seniority in appointing officers will enhance the quality of the Ministry's disaster management initiatives. The short institutional memory of administrative cadre staff rotated from other ministries will weaken the accumulation of disaster management wisdom gained from experience and lessons learned. Adequate steps must be taken to protect the civil service from politicization and corruption.

3.1.3 Financial

The DMIC is significantly under-funded to achieve and sustain all of the objectives identified in consultation with stakeholders.

The capital costs to equip local-level GoB offices with computers and network connections are beyond DMIC resources to provide a comprehensive supporting infrastructure. DMIC designers will constrain its functionality and range according to the funds available.

Similarly, the operations and maintenance cost of data, systems, services and staff must be constrained to fit the budgetary provisions.

CDMP DMIC ICT Strategy

3.2 Initiatives and Incentives to Develop Information Sharing Capacity

Many of the obstacles to information sharing discussed in the previous section can be removed or reduced. Some solutions are straightforward but others depend on attitudinal change.

3.2.1 Technical

ICT capacity required to fill the gaps in computerization and network infrastructure identified in the previous section is mainly beyond the resources of CDMP. However, CDMP can encourage the GoB to hasten the capacity development that it has already undertaken to provide. For example, GoB implementation of its commitment to propagate computer systems and internet connectivity to its offices down to the upazila level is overdue. CDMP should exploit opportunities to reinforce the understanding of GoB officers at all levels of the advantages of e-governance resources and of GoB dependency on ICT implementation to achieve many objectives. In particular, CDMP should maintain its lobby in the Ministry to advance this priority with the Ministry of Finance and its institutions that affect resource allocation, such as the Economic Relations Division and the Planning Commission.

CDMP should incorporate office automation skills training in its capacity building activities, with courses that encourage institutional use of email, file servers, collaborative office software and data management tools. Training material of all kinds should present concepts reflecting modern office practice wherever relevant, to reinforce the importance of the profound cultural shift that the Bangladesh institutions have to make.

The Bangla-English issue is an inherent feature of the operational environment. English will remain the language of technical communication and Bangla will always be the language of community interaction. Translation causes distortion, delay and complexity and is a fact of life. Requirements for translation can be reduced in database implementation by encoding field values numerically where possible. However, CDMP should not underestimate the accommodation it has to make to overcome this obstacle.

3.2.2 Institutional

Information sharing has to be a win-win situation for the parties involved. CDMP should clarify the advantages to each party of contributing or accepting the information. Some institutions, such as the Bangladesh Meteorological Department, are bound by their charter to share their information and need only consider their duty to be convinced. Others, like the Water Resources Planning Organization, may not be so mandated and may require payment for cost-recovery. In each case, CDMP must discover how to motivate information sharing that supports the objectives of the DMIC and its stakeholders. Section 3.3 describes how Memoranda of Understanding can stabilize inter-institutional information sharing.

In principle email can do all that a hand-carried signed letter does and more, and much faster, but hardcopy letters remain the preferred medium of the civil service. Few Government officers have a computer dedicated to their use or an email address. If GoB agencies are to productively share disaster management information, their staff must be equipped to access it, given office automation training and encouraged to make the DMIC portal their home page.

The mission, policies and operating procedures of each GoB institution should be documented, updated as necessary, made accessible to its entire staff and periodically audited to maintain consistency between documented procedure and practice. This will

CDMP DMIC ICT Strategy

empower officers to make correct local decisions with local information and relieve their superiors of the need to micro-manage. Staff should be appointed according to their qualifications, competence and performance so that they are capable of adequately executing the operating procedures. Satisfactory technical career paths should be established to encourage longevity and continuity in disaster management functions, to preserve institutional knowledge and leverage the benefits of lessons learned.

3.2.3 Financial

CDMP will continue to encourage donors to support the objectives of the DMIC development phase. However, in the longer term, a viable DMIC must establish reliable funding sources that meet its ongoing operational and incremental expansion needs. Section 4.7.3 describes approaches for sustainable funding of operations.

3.3 Data Sharing Agreements

Data is a dynamic commodity that reacts to pressure for change on the supply and the demand side. To meet institutional needs on both sides, discipline in the form of an interface specification, or Memorandum of Understanding must be imposed to formalize change so that the sharing parties maintain consistent performance borne of a common understanding of their obligations in the agreement.

A process for establishing an instance of information sharing should include the following steps:

1. identify a need for an information product
2. identify each of its data constituents in terms of:
 - o ownership, source
 - o stability, or rate of change
 - o format
 - o cost to user
 - o quality parameters: completeness, accuracy, time limitations
 - o intellectual property conditions
3. prepare information sharing agreements to secure the ongoing availability of the data

A model for information sharing should address these elements:

- a stable information product or products
- good will between the sharing parties at all levels
- a Memorandum of Understanding between the parties which:
 - o identifies the parties
 - o identifies the data to be shared
 - o specifies the data structure, accuracy and time validity
 - o specifies intellectual property conditions
 - o specifies payment terms, if any
 - o specifies the duration of the agreement
 - o specifies a quality assurance process
 - o specifies the process for renewing the agreement
 - o identifies the institutional points of contact for day-to-day issues
 - o identifies the institutional authorities responsible for the agreement

CDMP DMIC ICT Strategy

Table 3-1 lists some of the institutions with which the DMIC must formalize data sharing agreements.

Table 3-1 Necessary data sharing partners

Institutions	Data	Purpose
Bangladesh Bureau of Statistics	demographical	support vulnerability assessment
Bangladesh Meteorological Department	meteorological forecasts	<ul style="list-style-type: none"> • acquire meteorological and seismic data • disseminate hazard warnings
Center for Environmental and Geographic Information Services	flood and erosion predictions	<ul style="list-style-type: none"> • generate main river and flood plain flood warning information • generate erosion monitoring and prediction information
Ministry of Water Resources	flood and erosion warnings	disseminate hazard warnings
Flood Forecasting and Warning Center (BWDB)	water level predictions	<ul style="list-style-type: none"> • monitor main river water levels • generate main river water level predictions
Hydrology (BWDB)	bathymetric and hydrological	support erosion modeling
Institute of Water Modeling	flood and erosion warnings	<ul style="list-style-type: none"> • generate main river and flood plain flood warning information • generate erosion monitoring and prediction information
Survey of Bangladesh	topographical	support flood extent modeling
Water Resources Planning Organization	National Water Resources Database layers	support vulnerability assessment

Appendix A outlines a Memorandum of Understanding for data sharing between DMIC and other agencies.

CDMP DMIC ICT Strategy

4 ICT IMPLEMENTATION

4.1 Incremental Development

The DMIC functionality expected by stakeholders cannot be implemented in a single effort. Some elements are prerequisites to others; some depend on skills or data that DMIC users do not yet possess; some require ICT infrastructure that is not yet in place; and some may be infeasible until enabled by a new technology. An incremental approach conscious of these constraints will build the DMIC to provide the most necessary and feasible elements soonest and minimize risk of user disappointment. Figure Figure 4-1 suggests a possible DMIC development schedule, discussed in subsequent sub-sections.

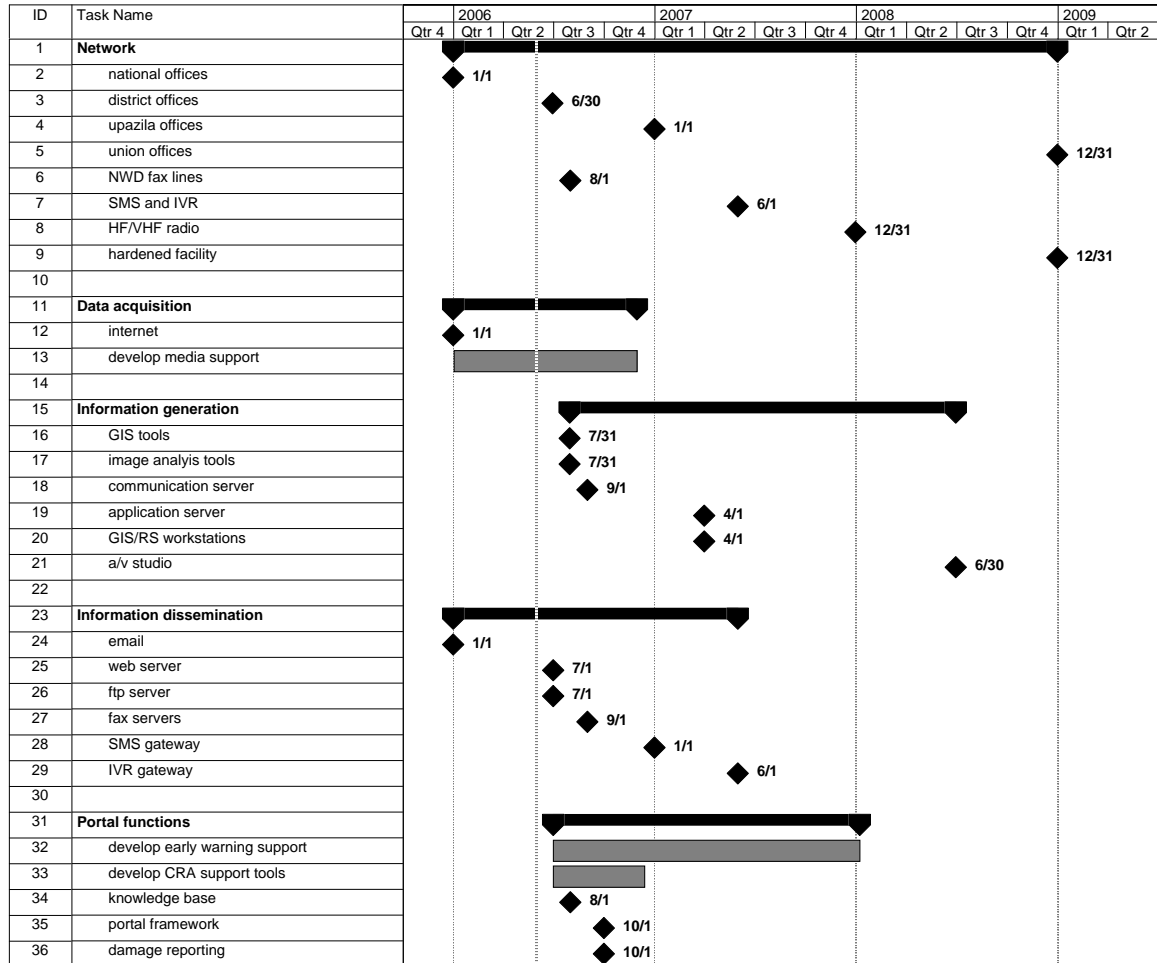


Figure 4-1 A possible DMIC development schedule

4.1.1 Data acquisition

From the beginning, DMIC peripherals should accommodate all of the common physical media, including floppy disks, CDRoms, DVDs, Digital-Audio Tape, and USB storage devices. A digital image scanner is required.

The internet will meet most needs for data acquisition by providing web interfaces, email and ftp. Consequently early emphasis on improving users' internet connectivity with the DMIC will have the most leverage. Important external sources of information that are not

CDMP DMIC ICT Strategy

adequately connected to the internet, such as the Bangladesh Meteorological Department, will need ICT capacity development.

When the above media have been made available, the following can be incrementally installed as required:

- SMS server and gateway
- IVR server and gateway
- audio and video studio facilities

4.1.2 Information Generation

In general initially the DMIC will provide information just as it receives it, without processing. However, exceptions will increase as users express requirements for information products that, for various reasons, only the DMIC can generate. The DMIC will make products that are composites of data from several sources, and that correct problems in source data. DMIC technical staff will use image analysis and GIS tools to develop these products. They will put GIS functionality in web applications that automate production and provide users with on-line GIS tools to manipulate data. The operational production of information should be simple, and automated to the fullest extent possible for daily execution by lower-skilled operators, while still affording flexibility for reconfiguration by senior technical staff.

Consequently, the DMIC will have spare processing capacity at an early stage to support these activities. At first, one workstation with software development, image analysis/editing and GIS development tools will be available, with capacity for expansion to several more.

4.1.3 Information Dissemination

The DMIC will begin its life cycle with certain fundamental information dissemination facilities. Because fax still predominates in institutional information transmission, the DMIC will have fax transmission and reception capability. However, fax machines are problematical in several senses: in transmission mode they have to be attended by a human operator; being mechanical they are inherently unreliable; the original image must first be printed and then may have to be physically stored for traceability of transmission; recovery from failed transmissions may be awkward; distribution lists are not easily maintained. An implementation based on fax modems and software servers integrated with product generation systems, and distribution and archiving achieved by means of database queries, avoids these problems. The DMIC will have this capability immediately.

As the institutional culture matures and users become more accustomed to and reliant on email and other digital media, the DMIC should develop these capacities, and in its capacity as an e-governance catalyst, it should have them at an early stage. Already some stakeholders prefer these media to fax, so the DMIC will support them from any early stage.

The DMIC will generate time-sensitive information items such as early warnings, situation reports and other real-time data, and present them in information products delivered through media that introduce least delay, consistent with the capacity of users to receive and comprehend them. Traditionally, early warning information originates in central institutions like BMD and FFWC, propagates by fax to district and upazila offices, and continues down the administrative hierarchy in hand- and voice-carried bulletins to the community. This traversal erodes prediction lead time, often entirely, and a single broken link starves all of the nodes below it so that some communities may not get the message at all. Mass media, especially state-operated media, broadcast early warnings directly to

CDMP DMIC ICT Strategy

communities throughout the country, but necessarily due to time constraints they aggregate the information to the extent that it is no longer as localized as it began or should usefully be. The DMIC will implement an alert subscription system in which local users can register to receive email, SMS or IVR early warning messages automatically composed to address the user's location and hazard concerns.

4.2 Training

Table 4-1 outlines the training required by classes of DMIC users and gives an indication of the number of users that will need training. However, the training activity can never be complete since staff turns over and new incumbents have to be trained. The training material should be of a quality that can be revived and reused.

Table 4-1 DMIC user training

Users	Qty	Required Training Course Content
DMIC staff		
Operations Manager	1	DMIC operations, user information needs, product generation and dissemination, portal maintenance
GIS/RS specialist	1	
DBA	6	
Operators	1	
QA Specialist	1	
System Administrator	1	DMIC operations and maintenance, user information needs, product generation and dissemination, portal maintenance
System technicians	2	DMIC maintenance, DMIN topology
CDMP staff	15	CRA tools, SOD, DMIC information products, portal functions
DRR staff		
HQ staff	10	CRIMS, SOD and its required outputs, DMIC portal functions and information products
DC staff	64	
DRROs	64	
PIOs	500	
Other GoB Staff		
DMB staff	10	SOD and its required outputs, DMIC information product generation, operations and portal functions
MoFDM staff	10	
EOC staff	6	
other agencies with SOD roles	100	SOD and its required outputs, DMIC information products and portal functions
other GoB staff (data providers)	10	SOD, DMIC operations and portal functions, user information needs, product generation and dissemination
other GoB staff (data users)	500	SOD, DMIC portal functions and information products
Other users		
NGO contractors	100	CRA tools, SOD, DMIC portal functions and information products
NGO data users	500	DMIC portal functions and information products
donors	10	

4.3 System Architecture

Figure 4-2 shows a strawman hardware architecture for the DMIC. Implementers should not be constrained to deliver the system as represented here; it is simply a starting-point for design consideration.

The DMC offices in districts, upazilas and unions will be connected through the internet with the DMIC, like other stakeholders. Important data providers and GoB agencies that

CDMP DMIC ICT Strategy

have emergency response control functions will have microwave links to the DMIC, and a redundant internet connection. Separate HF/VHF radio facilities may be installed.

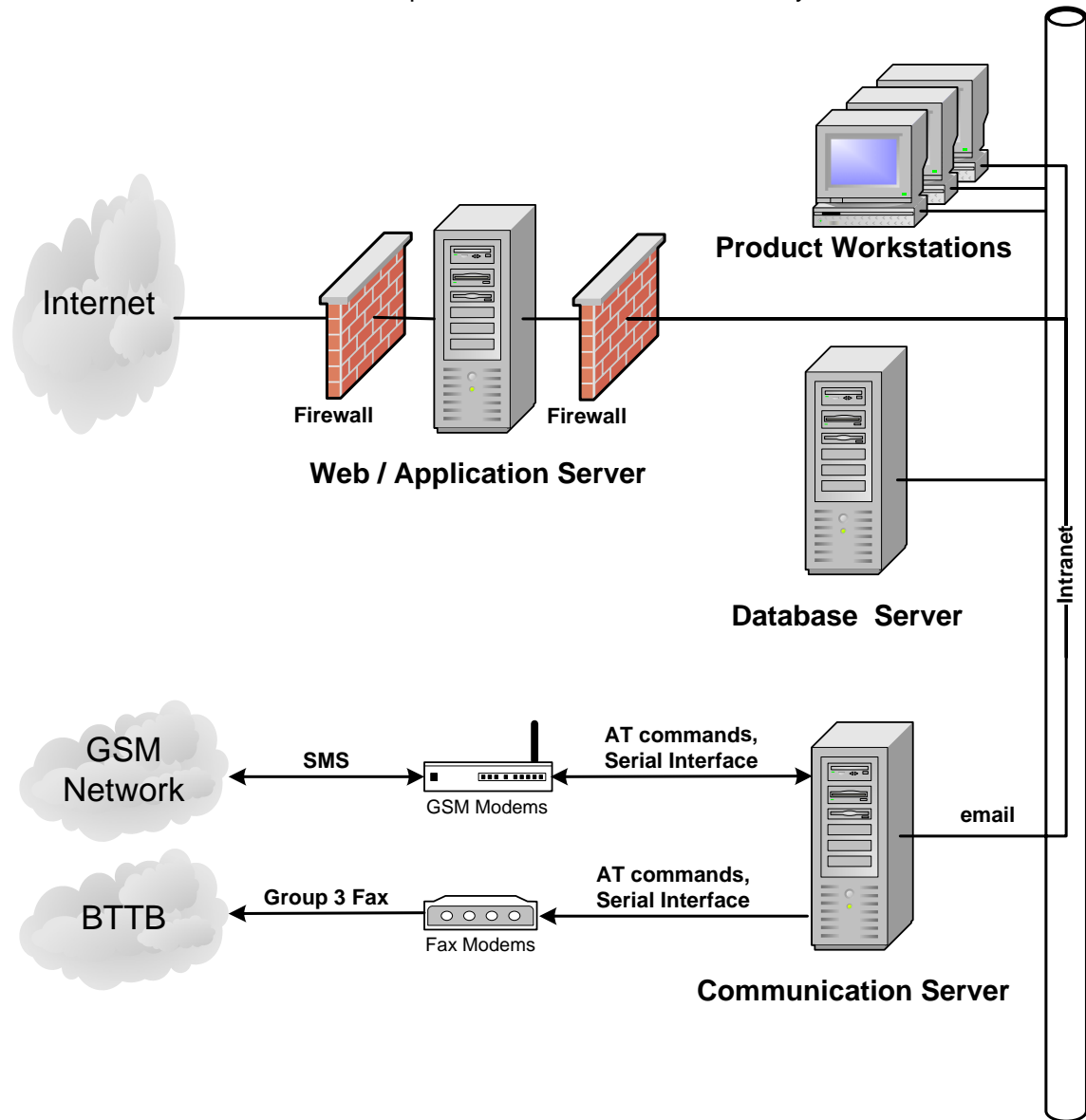


Figure 4-2 Strawman DMIC hardware architecture

A Local Area Network connects the following DMIC elements.

The **Product Workstations** provide GIS, image manipulation and computation tools for product generation. They also display human interfaces to the dissemination resources on the other computers. Most system operations are controlled through them.

The **Web/Application server** is the gateway to the internet. It hosts the httpd server that sends and receives http documents, and the application servers that act on data in those documents to retrieve records from the Database Server, do computations, present information to users logged onto the DMIC and interact with dissemination tools according to the programmatic logic. The portal framework is an important application that this machine hosts to present the DMIC functional interfaces to users on the internet.

CDMP DMIC ICT Strategy

The **Database Server** hosts most of the DMIC data, including GIS datasets, user information, knowledge base contents, and data for many other DMIC portal functions.

The **Communication Server** hosts applications that enable dissemination and acquisition of information through SMS, IVR, fax and email.

4.4 Network Requirements

This work is not yet done. The scope of the work is “Analyze the Network requirements in terms of connectivity, bandwidth, availability, scalability and flexibility, security and performance and prepare a five year action plan.”

4.5 Implementation Costs

The scope of this strategy document does not reflect the timing of availability of funds necessary to implement the strategy. The analysis assumes that funds will be provided in a timely series of payments that corresponds to the reasonable incremental development of the DMIC.

4.5.1 Equipment

Table 4-2 lists the DMIC equipment to be procured in the scope of this strategy, according to a preliminary analysis. These capital costs are approximate.

Table 4-2 DMIC equipment costs

Item	Qty	Unit Cost (BDT)	Cost (BDT)
DMIN infrastructure			
computers	235	80000	18800000
printers	235	30000	7050000
scanners	235	5000	1175000
modems	235	4000	940000
UPSs	235	6000	1410000
antivirus software	235	6000	1410000
MS Office	235	5000	1175000
DMIC infrastructure			
web/application server	2	120000	240000
communication server	2	350000	700000
workstation	3	120000	360000
GIS software	1	3000000	3000000
Oracle Portal suite	1	3250000	3250000
fax server software	1	14000	14000
plotter	1	300000	300000
digitizing table	1	100000	100000
colour printer	1	300000	300000
copier	1	300000	300000
GSM/EDGE modems	5	100000	500000
broadband modems	2	10000	20000
fax card with 4 modems	1	10000	10000
21" monitors	3	40000	120000
LCD projector and screen	1	200000	200000
firewall routers	3	500000	1500000
routers	15	50000	750000

CDMP DMIC ICT Strategy

Item	Qty	Unit Cost (BDT)	Cost (BDT)
UPS Online	8	400000	3200000
backup generator set	1	1000000	1000000
NWD lines	4	10000	40000
ISD line	1	20000	20000
mobile data connections	4	5000	20000
GPS instruments	5	25000	125000
microwave network links	15	200000	3000000
TOTAL (BDT)			5,10,29,000

4.5.2 Operations

Table 4-3 lists approximate service and consumables costs of the first three years of DMIC operations.

Table 4-3 Estimated 3 year cost of services and consumables

Services and Consumables		monthly cost	3 year cost
dialup internet connections	235	1000	8460000
broadband internet connections	2	30000	2160000
NWD lines	4	4000	576000
ISD line	1	10000	360000
mobile data lines	4	1000	144000
consumables and spares	1	10000	360000
TOTAL (BDT)			1,20,60,000

Table 4-4 estimates the three year labour costs of staffing the DMIC.

Table 4-4 Estimated 3 year DMIC labour costs

Labour	No.	monthly salary	duty time			3 year cost
			2007	2008	2009	
Operations Manager	1	60000	1	1	1	2160000
System Administrator	1	50000	1	1	1	1800000
GIS/RS Specialist	1	40000	0.5	0.5	1	960000
Database Administrator	1	40000	0.5	0.5	1	960000
Quality Assurance Specialist	1	25000	0.5	1	1	750000
Operators	6	20000	0.7	0.7	0.7	3024000
System Technicians	2	20000	1	1	1	1440000
TOTALS (BDT)						1,10,94,000

4.5.3 Training

Table 4-5 estimates the costs of the training described in Section 4.2 in terms of effort to prepare, effort to train trainers, effort to present one instance of the training and the numbers of likely trainees. Training material produced in preparation includes lesson plans, lesson material and user documents.

CDMP DMIC ICT Strategy

Table 4-5 Training costs

Courses	Preparation (pd)	Train the trainer (pd)	Presentation (days)	No. of Participants
CRA tools	10	12	2	120
CRIMS	10	60	2	650
DMIC operations	15		1	20
DMIN topology	5		0.5	5
information product generation	5		1	20
information products	3		0.5	20
portal functions	5	100	1	2000
product dissemination	3		1	20
SOD	20	300	3	2000
system maintenance	10		1	3
system operations	5		1	20
user information needs	2		0.5	20
Totals	93	472	14.5	4898

4.6 Design Considerations

This section is a discussion of qualities and characteristics that the DMIC design should address.

Usability

The DMIC will be staffed by officers of the Ministry with a wide range of technical competence. The duration of their employment in the DMIC in some cases may be short. Therefore operations should not depend heavily on staff competence, creativity and initiative but rather on built-in system intelligence and easy-to-use intuitive interfaces that staff can master with simple training.

Interoperability

Data will come from many sources and in many formats. The DMIC architecture may include several operating systems, eg, Windows 2003 Server and Linux. Interface design should anticipate interaction of various internal and external systems.

Maintainability

The DMIC will evolve from its first-increment design through states that are not well defined now. Its architecture should build on modular elements with minimal coupling and small well-defined interfaces to accommodate change with small impact on other system elements.

CDMP DMIC ICT Strategy

Reliability	<p>The DMIC needs to operate with very little down-time, with no early warning dissemination failure events lasting more than 4 hours, one event of between 0.25 and 4 hours and 10 events of less than 15 minutes per year. To achieve this reliability (99.9% up-time), the following design features should be included:</p> <ul style="list-style-type: none">• redundant communication media• independent internet services, one offshore• independent long-duration backup power
Survivability	<p>Hazards such as severe earthquake or local flooding may affect the physical premises of the DMIC. The DMIC should be equipped to survive hazards including seismic energy and prolonged disruption of public services such as security, water, food and power.</p>
EOC mirror	<p>The Emergency Operations Centre in the MoFDM should be equipped to access DMIC information.</p>
Presentation resources	<p>Large-screen monitors or projections in the DMIC operations room would be useful to display large and detailed GIS products and make presentations to visitors.</p>
Domain name	<p>The DMIC portal should have a .gov.bd domain name to reflect the authority of the Ministry behind the information that the DMIC provides.</p>

4.7 Sustainability

Sustainability is an essential element of development success. Too many endeavors begin well, meet their project-phase objectives, and decline after the donor organizations withdraw. Sustainability is a quality of systems that remain viable to achieve their missions throughout their planned operational lives, by securing on-going technical, institutional and financial resources. The following sections suggest approaches that the DMIC should take to address lessons learned from the successes and failures of other developed systems.

4.7.1 Technical

Technical sustainability protects the system from failure due to technological weaknesses. Historically, systems have often failed because the equipment ceased to function adequately in the absence of the highly-skilled or expensive maintenance resources that were available during the development phase.

The lessons learned for system design are:

- make a system that is easy to operate, maintain and change
- use reliable, robust and long-lived equipment that tolerates the operational environment
- minimize requirements for expensive or difficult-to-obtain consumables such as coloured inks and special paper.

Get adequately competent system operations staff:

- expect and make allowances for turnover
- maintain job descriptions with required qualifications, skill sets
- encourage staff longevity by

CDMP DMIC ICT Strategy

- showing a career path
- offering better than average pay and benefits
- maintaining a good work environment
- operate an effective, repeatable staff training program.

Establish ways to accumulate and preserve corporate knowledge:

- Encourage a documentation culture
- Provide system resources for easy creation, maintenance, storage and retrieval of knowledge
 - System design
 - System operations
 - Training materials

Use information products and media that are within users' capacity:

- verify that users receive and use information products effectively
- adjust the products and media according to user feedback.

4.7.2 Institutional

A useful practice that fits the culture of an institution, and does not conflict with its other practices, thrives if given resources. Institutional sustainability depends on the will of the organization to support the practice. The DMIC should endeavor to fit itself to the disaster management community, in particular, to the agencies of the Ministry, with little expectation to change institutions to fit the system. However, the DMIC is an ICT development consistent with the e-governance intentions of the Government of Bangladesh and should expeditiously advocate the benefits that ICT is bringing to the rest of the world.

MoFDM, DMB and DRR staff should operate the DMIC from as early a stage as possible so that when CDMP completes, the DMIC is fully integrated in the GoB and does not depend on external resources.

The DMIC should use existing institutional dissemination mechanisms as much as possible and resist the temptation to make new media where the traditional ones are adequate.

The DMIC should pay constant attention to stakeholders' needs for appropriate information, media and training, and give them what they want. Needs assessment never ends. Stakeholders' perceptions of their needs change with awareness of the possibilities.

The DMIC should establish processes to create, maintain and enforce information sharing agreements. Memoranda of Understanding are essential for stabilizing the chaotic expectations of the diverse and numerous stakeholders in the disaster management community.

4.7.3 Financial

A business plan will be prepared which examines financial issues in more detail. The key problem is narrowing the gap between required and available resources in a dynamic environment. The obvious parallel solutions are to reduce costs and increase funding.

The DMIC can reduce operations and maintenance costs by:

- keeping operations simple to minimize personnel costs
- procuring reliable equipment to minimize maintenance costs

CDMP DMIC ICT Strategy

- procuring efficient services to minimize communication costs
- minimizing use of paper to reduce cost of consumables

Approaches to acquiring funds for DMIC operations include:

- entrenching ministry revenue budget items to fund basic operations
- selling information subscriptions to donor agencies
- selling advertising on the portal

CDMP DMIC ICT Strategy

5 DMIC MANAGEMENT PLAN

5.1 Operational Scenarios

Since some hazards occur independently of season and hour, DMIC will operate continuously throughout the year and around the clock. MoFDM officers will staff DMIC activities in normal times and emergencies to accomplish the operational tasks described in this section. Elaboration of operating procedures is premature before the design stabilizes but general discussion of operations is helpful now to expose issues that can be addressed in design.

5.1.1 Normal operation

This section outlines the day-to-day tasks that must be completed even in the absence of emergencies, to maintain the service quality of the DMIC and its readiness to meet user expectations in normal and emergency times. The operation of the DMIC in Mohakhali, its mirror in the Ministry of Food and Disaster Management and its network nodes in DRROs and upazila PIO offices are continuous activities that will occupy the entire staff. Table 5-1 outlines the DMIC operational activities.

Table 5-1 DMIC daily operational activities

Operations management	The Operations Manager responds to direction from the Chief Executive Officer and directs the DMIC staff accordingly. (S)he also: <ul style="list-style-type: none"> • reports technical, production and financial status to the CEO • manages human, infrastructure and financial resources • liaises with DMIC stakeholders to manage their expectations • plans and supervises DMIC expansion and product development • maintains the 24-hour Operator staffing schedule • maintains the product generation and dissemination schedule
Information sharing	The Operations Manager liaises with information partners and creates/modifies MOUs according to the needs of the parties and their common understanding of the terms of the relationships.
User management	Operators review new user registrations for compliance with membership criteria. They validate addresses in distribution lists and check consistency of access control lists with the security rules.
Data acquisition	The GIS/RS Specialist and Database Administrator maintain the regular sources of early warning information, from BMD, FFWC, CEGIS and other institutions, ensuring that the daily data are available and corresponding products are available for dissemination. They procure data as needed from other sources, such as BBS, NWRD, SoB and MoA.
Product development and maintenance	The Operations Manager requests and receives feedback from users on current products and media. The DMIC development team (Operations Manager, GIS/RS Specialist, Database Administrator, System Administrator and QA Specialist) mock up new/changed products and field test them. They design and test new production and dissemination procedure, and roll out new products and media.
Product dissemination	The Operators perform manual operations and ensure that automated operations complete, to disseminate information products to users according to their preferences. They update portal content. They send hardcopy products using courier/postal delivery.

CDMP DMIC ICT Strategy

System maintenance	The System Administrator and Technical Specialists continue the DMC network expansion. They maintain network, processing and data storage equipment and inform the QA Specialist of system changes. They monitor and tune system performance and network security functions. Operators replace system and user data backup tapes.
Software maintenance	The System Administrator ensures that software licences are current and compliant. (S)he acquires and installs upgrades as necessary, configures software appropriately, creates/revises custom software, provides user support for new software and services and informs the QA Specialist of system changes.
User support	The Operations Manager liaises with the PMO, MoFDM, DMB, DRR and major information providers. The System Administrator and Operators resolve users' technical problems in CDMP, at the DMC nodes and in external agencies. In general they interact with users through an online problem reporting system that has web and telephone interfaces.
Quality assurance	The QA Specialist reviews input data from information providers and products generated by DMIC for dissemination to users, for compliance with the terms of the corresponding MOUs. (S)he reports discrepancies using the problem reporting tool for disposition by the Operations Manager. The QA Specialist ensures that DMIC documents, software, data and hardware items are identified in a database with their name, version and location, and are retrievable from the recorded location. (S)he verifies that no changes to the items are made without the approval of the System Administrator. The QA Specialist tests system changes to ensure that the system continues to operate in compliance with its requirements.

5.1.2 Emergency operation

In times of emergency, many of the normal operations described in the previous section must still be completed. Specifically, activities on which reliable system performance depend, such as liaison with information providers, technical support to users and quality assurance, continue. Table 5-2 outlines additional activities are crucial to maintain effective support of emergency response in a dire and chaotic disaster environment.

Table 5-2 DMIC emergency activities

System testing	Frequent testing of media connectivity will reduce the risk of prolonged interruption of DMIC support by alerting the operator to the need to fix problems or provide alternate information routing.
Moderate blogs	The forum tool available to enable free-form sharing of situation reports, actions and intentions of responders has to be monitored for misleading and inconsistent information. Operators should moderate the inputs and take action to verify them to resolve any inconsistencies, ambiguities and errors that they find.
Validate information	Operators will attempt to check information from unfamiliar single-sources to reduce the risk that responders take wrong actions based on erroneous items published on the DMIC.
Search for information	When needed information items are absent or stale, the Operators will search for current information.
Respond to requests	Operators will respond to external requests for information.

CDMP DMIC ICT Strategy

5.2 DMIC Staffing

This staffing plan assumes around-the-clock, 365 days per year operation of the DMIC. The functions it describes are essential because that work must be done; otherwise the DMIC will not achieve its goals. To some extent job description elements of two or more functions might be allocated to a single person, with the risk that they will not be adequately executed due to insufficient capacity of that person to complete the work.

For example, two people may be able to provide the functions of the Operations Manager, GIS Analyst, Database Administrator and System Administrator. No reduction in Operators is possible if the Centre is to be attended around the clock. Similarly, the geographical scope and technical demands of supporting upazila nodes throughout the country require two technicians. The Quality Assurance Specialist must not have operational responsibilities because that person has to remain independent of the work to be able to assure its quality.

Preliminary analysis suggests that two System Technicians will be sufficient to maintain the remote DMIC nodes in district and upazila centres. For 24/7 operations, six Operators will staff a rotating roster of three daily eight-hour shifts, allowing for vacation, sick time and other causes of brief intervals of under-staffing.

CDMP should attempt to fill DMIC positions with MoFDM staff.

5.2.1 Organization

Figure 5-1 shows the functional organization of DMIC staff.

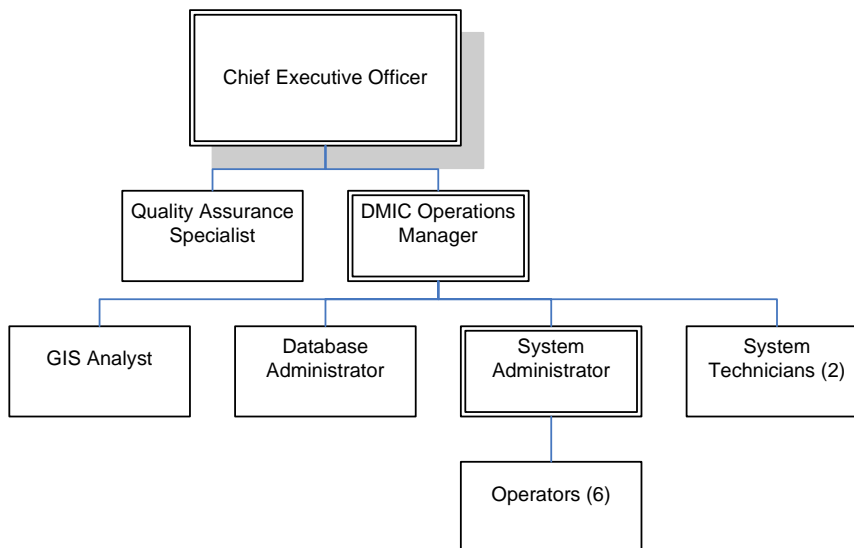


Figure 5-1 DMIC operations staff organization

CDMP DMIC ICT Strategy

5.2.2 Job descriptions

Chief Executive Officer	<ul style="list-style-type: none">• responsible for DMIC operation• arbitrates quality issues that are unresolved at lower levels
Quality Assurance Specialist	<ul style="list-style-type: none">• reports to CEO• assesses input data and output product quality• assesses processes with respect to DMIC Operations Plan• tracks problem reports and corrective action• assures change control and configuration management• tests system changes• escalates unresolved quality issues to CEO
Operations Manager	<ul style="list-style-type: none">• manages staff• negotiates and maintains MOUs• provides external point-of-contact• plans and supervises incremental development• procures equipment and external services• reports to CEO• maintains budget and accounts
System Administrator	<ul style="list-style-type: none">• system/software engineer• supports incremental development• maintains portal• provides second-level technical support
GIS Specialist	<ul style="list-style-type: none">• develops and maintains GIS tools• maintains data• maintain products according to MOUs
Database Manager	<ul style="list-style-type: none">• develops and maintains database• maintains data consistent with MOUs• supports incremental development
Operators (6, part time) for 24/7 operations	<ul style="list-style-type: none">• answers the phone, responds to user email• verifies new user registrations• maintains user data• provides first-level technical support• executes periodic maintenance as per schedule, eg, backups• maintains portal content• executes manual operations tasks• calls System Administrator if necessary
System Technicians (2)	<ul style="list-style-type: none">• provides technical support for 235+ GoB network nodes• implements network expansion

CDMP DMIC ICT Strategy

A. Data sharing Memorandum of Understanding outline

Table of Contents

1	Parties to the Agreement
2	General
2.1	Purpose
2.2	Benefits
2.3	Definitions
3	Operations Plan
3.1	Activities
3.1.1	Agreement maintenance
3.1.2	Data sharing
3.1.3	Product generation
3.1.4	Product dissemination
3.2	Quality Assurance
4	Terms of Agreement
4.1	Completion Date
4.2	Termination
4.3	Participation in Similar Activities
4.4	Intellectual Property Rights
4.5	Financial
5	Signatures

Appendices

A	Input data specifications
B	Information product specifications
C	Distribution lists for information lists