Implementation Monitoring and Evaluation Division
Ministry of Planning
Sher-e-Bangla Nagar, Dhaka 1207, Bangladesh

Monitoring and Evaluation Guideline
on
ICT and Related Field

June 2019

Abbreviations and Acronyms

A2I	Access to Information
BBS	Bangladesh Bureau of Statistics
BCC	Bangladesh Computer Council
DC	Deputy Commissioner
CIRT	Computer Incident Response Team
DESC	District e-Service Centre
FGD	Focus Group Discussion
GDP	Gross Domestic Product
GED	General Economics Division
ICT	Information and Communication Technology
IMED	Implementation Monitoring and Evaluation Division
ITU	International Telecommunication Union
IO	Innovation Officer
KII	Key Informant Interview
M&E	Monitoring and Evaluation
MDG	Millennium Development Goal
MoU	Memorandum of Understanding
NESS	National e-Service System
PPA	Public Procurement Act
PPR	Public Procurement Rules
SDG	Sustainable Development Goal
SIF	Service Innovation Fund
SMECI	Strengthening M&E Capabilities of IMED
TPP	Technical Project Proposal
ToR	Terms of Reference
UDC	Union Digital Centre
UNO	Upazila Nirbahi Officer
UP	Union Parishad

Table of Content

Chapter VIII: Recommendation

Annexure

Executive Summary

Implementation Monitoring and Evaluation Division (IMED) is the apex body of the Government of Bangladesh to monitor and evaluate implementation of public sector development projects included in the Annual Development Programme (ADP). Through monitoring and evaluation IMED points out to project implementing ministries and other appropriate authorities the progress of implementation and problems encountered, if any, in the field relating to quality, time, cost etc. for taking remedial measures.

For the purpose of carrying out field review a comprehensive guideline is necessary. Therefore, IMED intends to develop a Monitoring & Evaluation Guideline on ICT and Related Field for the use IMED officers. Since ICT part is considered thrust sector of the economy. Government substantial allocation of the annual development budget, its development activities have attracted greater attention of the government and that demands more focused and intensive quality monitoring by the IMED. Information & Communication Technology (ICT) is one of the most important tools to achieve economic prosperity of a country through improving the management and efficiency in every sphere of life. The experience of the developed and emerging economies supports the notion. The purpose of ICT is to improve Growth, Employment, and Governance for Bangladesh.

In the guideline key components of ICT projects that are being addressed are Software, Hardware, Networking, Mobile based Application, 4th Generation Technology, Security, Training, Repair and Maintenance, Warranty, Documentation, Testing and Post-Implementation Evaluation.

Monitoring and evaluation guideline been prepared for different ICT components such as application software which is designed to help the user to perform specific tasks like enterprise resource planning, accounting, office suites and graphics software etc. Applications may be bundled with the computer and its system software, or may be published separately. In recent years, the abbreviation "app" has specifically come to mean application software written for mobile devices. The executing agencies shall comply the minimum requirements while acquiring software such as Total Lifecycle Cost, Maintainability, Interoperability, Portability, Scalability, Availability, Accessibility, Reusability, Functionality, Performance and Security.

Where IT equipment or products exhibit some of these characteristics, it shall be considered non-compliant: The product is not complete and some essential parts are missing; Functionality or safety is impaired; The appearance is generally worn or damaged; It is destined for disposal or recycling instead of use; and It is old or outdated destined to be cannibalized to gain spare parts.

In this guideline there are suggested specifications for Hardware, Cloud Computing, Website and Data Center. Also there are checklist for Web Applications, Information Security Documentation, Incident Response Plans, Vulnerability Analysis, System Continuity and Disaster Recovery; Servers and Network Devices; Software Application Development and Access Control.

The guideline describing all the steps for handling procurement of ICT Services is developed with a view to monitor and evaluate implementation of ICT components. It would also enable the procuring agency to monitor the responsibility of executing procurements in accordance with the Government procedures.

CHAPTER ONE
Study Background

1.1 Background of the Study

Implementation Monitoring and Evaluation Division (IMED) is the apex body of the Government of Bangladesh to monitor and evaluate implementation of public sector development projects included in the Annual Development Programme (ADP). Through monitoring and evaluation IMED points out to project implementing ministries and other appropriate authorities the progress of implementation and problems encountered, if any, in the field relating to quality, time, cost etc. for taking remedial measures. For timely and proper management of these activities along with the main functions a comprehensive strengthening program has been gravely felt for long time. Therefore, IMED has undertaken the development project, entitled "Strengthening M&E Capabilities of IMED (SMECI)" funded by the GoB.

An important function of IMED is to carry out regular field inspections of development projects to keep itself abreast with the latest progress of projects in the field. It informs the relevant ministries and agencies with the impending problems as well as current problems affecting the progress of projects, for taking corrective measures at their end, so that project's physical and financial progress are accelerated.

ICT is one of the most important tools to achieve economic prosperity of a country by improving management and efficiency. ICT is considered as a thrust sector of the economy. Government has allocated substantially for ICT in the annual development budget, and that demands more focused and intensive quality monitoring by IMED. For the purpose of carrying out regular monitoring a comprehensive guideline is necessary. Therefore, IMED intends to develop a Monitoring & Evaluation Guideline on ICT and Related Field for the use IMED officials.

1.2 Objective of the Assignment

The main objective of the assignment is to prepare an M&E Guideline concerning important areas of ICT and Related Field projects, which will help as a tool for monitoring by IMED officials.

The specific objectives of the assignment are the following:

- To review existing available relevant documents/guidelines on project inspection;
- To review existing available relevant documents/guidelines of other relevant countries and development partner agencies;
- To analyse objectives of the assignments thoroughly;
- To develop a guideline that can be effectively used by IMED officials during project monitoring and evaluation;
- To develop an identical M&E template for relevant sector;
- To guide the officers of the IMED in building systematic approach to field visit through use of the Guideline;
- To ensure the project management knowledge areas (such as scope, time, cost, procurement, quality, integration, human resource, stakeholders, communication and risk);
- To help accelerate progress of the development projects.

1.3 Scope of Services

Consultancy services shall broadly include:

- Prepare a study design to carry out interviews of the stakeholders to know the actual requirement of ICT and Related Field (To address Science, Information and Communication sector related projects of Annual Development Program) connected projects for preparation of the guideline;
- Identify weaknesses and limitations in the monitoring and evaluation process of the related projects;
- Identify key areas of project development activities, and also identify select smart indicators for effectively monitoring and evaluating related projects;
- Identify the components of different development projects, and describe the parts of each component for effective monitoring and evaluation;
- Study monitoring and evaluation reports, in-depth study reports and other related reports of the projects of the concerned sector and identify monitoring and evaluation weaknesses etc;
- Study other relevant documents and M&E procedure of ICT and Related Field projects/program of in country and other countries that can be helpful In preparing M&E Guidelines;
- Consultant/s will interact with the relevant ministries, agencies, projects and identify areas of interest that can be helpful in carrying out the assignment;
- Consultant will deliver comprehensive M&E guideline and M&E templates for ICT and Related Field (To address Science, information and Communication sector related projects of Annual Development Program) in English and Bangla;
- Any other related works assigned by the client.

1.4 Responsibilities of the Consulting Firm

- The consulting firm must propose services of consultants having good academic background and knowledge of the subject (assignment), so that quality M&E Guidelines and templates can be prepared and delivered within the stipulated time frame;
- The consulting firm shall propose an appropriate methodology for the study in the context of objective of the assignment and scope of services;
- Prepare and finalize M&E Guideline based on the study of documents, objective of the assignment and the data/information collected from various internal and external sources. M&E Guideline should cover maximum areas of monitoring activities/ components of specific item;
- Arrange a Workshop/Seminar for dissemination of the study findings and finalizing the guideline incorporating comments/observations of the participants.

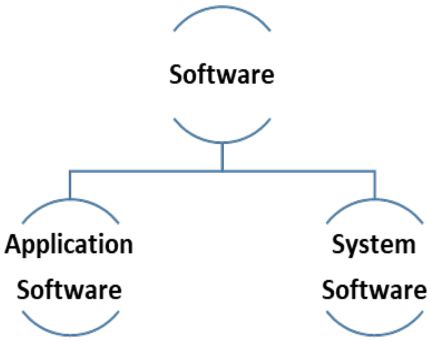
CHAPTER TWO
Software

2.1 Software

Software is a set of instructions, data or programs used to operate computers and execute specific tasks. Opposite of hardware, which describes the physical aspects of a computer, software is a generic term used to refer to applications, scripts and programs that run on a device.

2.2 Classification of Software

This guideline classifies software into two categories based on its purpose, functionalities, type, or area of application which is Application Software and Systems Software.



2.2.1 Application software

A program or group of programs designed for end users. Application software is mainly computer software designed to help the user to perform specific tasks like enterprise software, accounting software, office suites, graphics software and media players etc. Applications may be bundled with the computer and its system software, or may be published separately. In recent years, the abbreviation "app" has specifically come to mean application software written for mobile devices. Executing agencies shall take into consideration the following when acquiring application software:

i. Feasibility of the software for fulfilling agency's need;.
ii. Type of application to be used; desktop application, web based application or server application.
iii. Operating System platform the software to be developed is to run on.
iv. Integration with the existing systems (if any).
v. Database to be used by the application.
vi. Compatibility with existing and future hardware and software platforms.
vii. Speed of development.
viii. Performance of compiled code or programming tools to be used.
ix. Portability; can the application developed be used in an operating systems other than the one in which it was created without requiring major rework.

2.2.2 Development of Application Software

The development of application Software shall fall under the following measures

i. In house development

The development of all application software through in-house means shall be coordinated and guided by executing agencies. The executing agency will constitute a development team consisting of various specializations as may be required in specific software development task to provide support and expertise together with the task teams from other executing agencies.

ii. Outsourced Development

For sophisticated system development initiatives that require skills and knowledge not available within, an external developer/ IT firm may be contracted to deliver the application. The implementing agency outsource IT firm which constitute a technical team with the relevant IT skills to carry out the tasks.

iii. Commercial off-the shelf

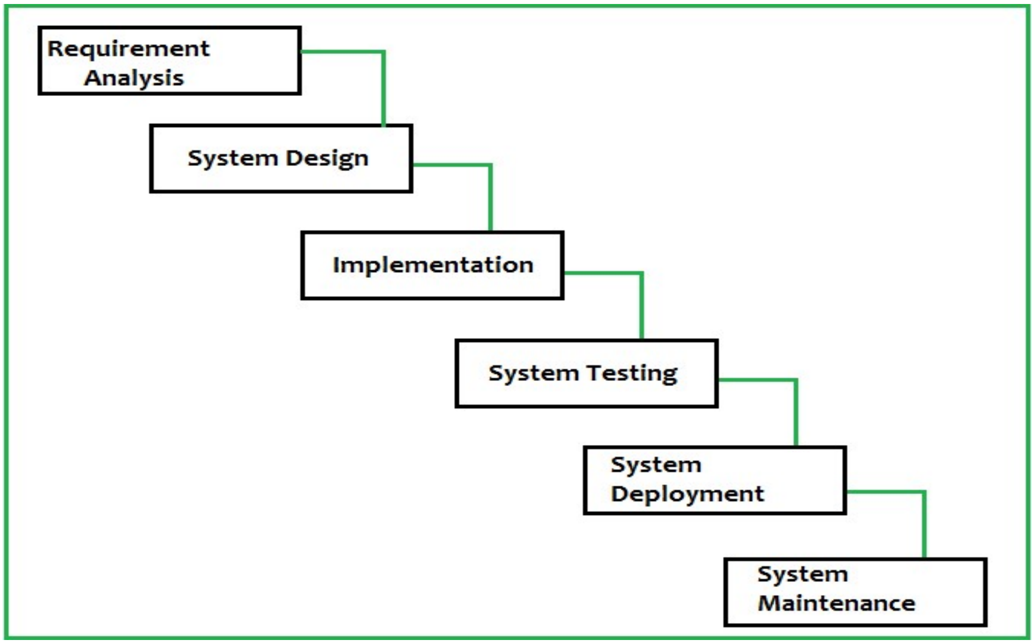
Commercial Off-the shelf software are readily available solutions in the market. Government executing agencies intending to acquire application software through these means shall ensure that the specifications are well detailed to meet the functional and technical requirements. Off-the-shelf or commercial software defines software which is ready-made and available for sale, lease, or license to the general public. Purchasing a commercial off-the-shelf software solution requires attention to technical and cost considerations.

2.2.3 System software

System software is software on a computer that is designed to control and work with computer hardware. It is a collection of operating system, servers, device drivers, utilities and windows systems which helps in running the computer hardware and the computer system. It is designed to provide a platform to run application software and operate the computer hardware. This software helps an application programmer to view away memory, hardware and other internal programme of a computer. Some system software is used directly by users and other system software works in the background. System software can allow users to interact directly with hardware functionality, like the device manager and many of the utilities found in the control panel.

2.3 Software Development Phases

The software development life cycle (SDLC) is a process used for structuring the development of any software system, from initiation through to implementation. SDLC is considered to be the foundation for all software development methodologies, with various activities associated with each level. Activities such as budgets, requirements gathering, and documentation writing, are included in the cycle, as well as the more technical elements. SDLC usually begins with determining organisational needs, which is followed by implementation and testing. For software development we have to emphasis on following issues to be covered. Different phases are to be monitored as listed below:



2.3.1 Requirement Analysis

Requirement analysis is one of the most important phase in software development and also in other ICT related development. Requirements analysis involves frequent communication with system users to determine specific feature expectations, resolution of conflict or ambiguity in requirements as demanded by the various users or groups of users, avoidance of feature creep and documentation of all aspects of the project development process from start to finish. The software requirements are description of features and functionalities of the target system. Requirements convey the expectations of users from the software product. Software requirements specification shows what the software is supposed to do as well as how it is supposed to perform. It is written down before the actual software development work starts. SRS ensures that there is less possibility of future redesigns as there is less chance of mistake on the part of developers as they have a clear idea on the functionalities and externalities of the software as well as client get the exact functionalities of the work as he wants. Here we define requirement analysis in four steps, which includes

i. **Feasibility Study**

When the client approaches the organization for getting the desired product developed, it comes up with rough idea about what all functions the software must perform and which all features are expected from the software. Referencing to this information, a detailed study should be done about whether the desired system and its functionality are feasible to develop. This study analyzes whether the software product can be practically materialized in terms of implementation, contribution of project to organization, cost constraints and as per values and objectives of the organization. It explores technical aspects of the project and product such as usability, maintainability, productivity and integration ability. The outcome of the technical feasibility study is to define the various technical approaches that can be followed to implement the project successfully with minimum risks. The output of this phase should be a feasibility study report that should contain adequate comments and recommendations for management about whether or not the software development in the project should be undertaken.

ii. **Requirement Gathering**

If the feasibility report is positive towards undertaking the project, next phase starts with gathering requirements from the user. Then analysts and developers will start communicate with the client and end-users to know their ideas on what the software should provide and which features they want the software to include.

iii. **Software Requirement Specification**

SRS is a document created by system analyst after the requirements are collected from various stakeholders. SRS defines how the intended software will interact with hardware, external interfaces, speed of operation, response time of system, portability of software across various platforms, maintainability, speed of recovery after crashing, security, quality, limitations etc. SRS should come up with following features:

- User Requirements are expressed in natural language.
- Technical requirements are expressed in structured language, which is used inside the organization.
- Design description should be written in Pseudo code.
- Format of Forms and GUI screen prints.
- Conditional and mathematical notations for DFDs etc.

iv. **Software Requirement Validation**

After requirement specifications are developed, the requirements mentioned in this document are validated. Requirements can be checked against following conditions -

- If they can be practically implemented
- If they are valid and as per functionality and domain of software
- If there are any ambiguities
- If they are complete within the stipulated time
- If they can be demonstrated

2.3.1.1 Defining Requirements

Once the requirement analysis is done the next step is to clearly define and document the product requirements and get them approved from the appropriate authority. This is done through an SRS (Software Requirement Specification) document which consists of all the product requirements to be designed and developed during the project life cycle. There are different types of requirement which we should consider to get a efficient product.

i. **Organizational Requirements (Opportunity)**

Organizational requirements are the goals, objectives, or needs which should help the organization to ensure cost effectiveness, minimize expenditures, raise service to a new level or meet the regulatory requirements. In line with documenting requirement we should focus on following issues.

- Project background
- Scope statement
- Requirements purpose
- Context diagram
- Objectives & benefits summary
- Organisational drivers/issues
- Dependencies
- Assumptions

- Constraints/restrictions
- Organisational transaction volumes
- Regulatory considerations
- Privacy impact assessment
- Records impact assessment
- Open issues

ii. User Requirements (Need)

User requirements are the requirements that should include the goals and objectives which the system will allow the users to achieve. They also cover the following issues

- Use case overview
- Process model
- Actor profiles & locations
- Inputs
- Outputs
- User interface
- Triggers
- Organisational rules
- Function hierarchy diagram & report
- Data flow diagram

iii. Functional Requirements (Product Capabilities & Behaviour)

The Functional Requirements Specification documents the operations and activities that a system must be able to perform. It describes how a product must behave, what its features and functions should be. They also cover the following issues

- Operational environment
- System interface
- Communications interface
- Software interface
- Hardware interface
- Function/user security matrix
- User group & system access summary

iv. Non-functional Requirements (Success Factors)

Nonfunctional requirements describe the general characteristics of a system. They are also known as quality attributes. They also cover the following issues

- Response/ performance
- Capacity
- Reliability
- Operability
- Maintainability
- Scalability
- Availability
- Delivery
- Recovery
- Transition requirements

v. **Data Requirements (Structure)**
  - Logical data model
  - Data conversion requirements
  - Warehousing
  - Data volumes & size
  - Data retention/archive/purge

2.3.2 System Design

SRS is the reference for product architects to come out with the best architecture for the product to be developed. Based on the requirements specified in SRS, usually more than one design approach for the product architecture is proposed and documented in a DDS (Design Document Specification). This DDS is reviewed by all the important stakeholders and based on various parameters as risk assessment, product robustness, design modularity, budget and time constraints, the best design approach is selected for the product. A design approach clearly defines all the architectural modules of the product along with its communication and data flow representation with the external and third party modules (if any). The internal design of all the modules of the proposed architecture should be clearly defined with the details in DDS.

2.3.3 Software Development

In this stage of SDLC the actual development starts and the product is built. The programming code is generated as per DDS during this stage. If the design is performed in a detailed and organized manner, code generation can be accomplished without much hassle. The programming language is chosen with respect to the type of software being developed.

2.3 4 Testing

This stage is usually a subset of all the stages as in the modern SDLC models, the testing activities are mostly involved in all the stages of SDLC. However, this stage refers to the testing only stage of the product where their defects are reported, tracked, fixed and retested, until the product reaches the quality standards defined in the SRS.

2.3.5 Deployment

Once the product is tested and ready to be deployed it is ready to be released formally. Sometimes product deployment happens in stages as per the strategy of that organization. The product may first be released in a limited segment and tested in the real environment (UAT- User acceptance testing). Then based on the feedback, the product may be released as it is or with suggested enhancements in the targeting market segment. After the product is released in the market, its maintenance is done for the existing customer base. UAT must be done and accepted by client.

2.3.6 Maintenance

The maintenance phase takes care of this activity by timely tuning the software as per the requirement.

2.4 Issues to be addressed for Software

The following are the minimum requirements that executing agencies shall comply with while acquiring software.

- **Total Lifecycle Cost**: This cost includes initial costs such as purchase, installation and training, plus the on-going cost of maintenance and support.

- **Maintainability**: Maintainability means fixing, updating, servicing and to modify the system or update the software for performance improvements or for the correction of faults. Maintainability also includes the addition of new functionality or the adaptation of software to meet new requirements for the customer needs. Software maintainability is the degree of an application to repaired or enhanced it. Maintainability increases the reliability, efficiency or safety of the software. It is also used to make future maintenance easier. It is used to increase the lifetime of the software. Maintainability repair or replace the faulty components and make the software even better as compared to the previous condition of the software.

- **Interoperability:** Interoperability is defined as the ability for computer software to communicate with one another for the effective exchange and process of information. There may be different software is used within an organization or outside that organization. For example nearly all hospital systems, clinics, pathology labs, and other institutions utilize different software. The importance of interoperability comes within the fact that in order to provide effective, comprehensive care to patients, medical professionals need to provide and receive access to medical records, histories and analytics in a centralized manner to enhance their practice, and utilize valuable data towards predictive analytics and intelligence in healthcare. This criterion seeks to minimize the additional support required to integrate with the product as a functioning component in the Government IT portfolio;

- **Portability:** This criterion addresses the ability of an existing software component to move from one physical or logical position in the IT infrastructure with minimum impact on cost and service; software portability that allow game software developers to make software for one system and deploy them across multiple platforms.

- **Scalability**: Scalability is an attribute that describes the ability of a process, network, software or organization to continue to function well when changes are done in the size or volume of the system to meet a growing need. Scalability is often a sign of stability and competitiveness, as it means the network, system, software or organization is ready to handle the influx of demand, increased productivity, trends, changing needs and even presence or introduction of new competitors. Online newspaper is getting popular day by day. And when users access the site, they expect to be directed to their newsfeed immediately and for the read and write functions to perform quickly. This scalability should be considered to make changes are done in the size or volume of the system to meet a growing need in action.

- **Availability/Accessibility**: This seeks to maintain a system's operational readiness and required level of service without disruption from software failure. This is achieved through robust and/or redundant (e.g., fault tolerant) software. Operational readiness will include the ability of users and operators to access the system, in a timely fashion, to perform its intended functions;

- **Reusability:** This criterion addresses the ability to make repeated use of the software product for additional requirements with minimum additional cost;

- **Functionality/performance:** This criterion seeks to guarantee that the e-Government Operational requirements, especially its mission critical requirements, intended to be performed by IT systems, can be achieved effectively and efficiently with the specified software. It includes the properties of efficient software/hardware integration that affects the ability of the overall system to perform adequately to meet operational requirements.

- **Security:** This criterion addresses the need to protect system data and the operational environment from loss or compromise. It includes the ability of the software to prevent and contain malicious as well as non-malicious security breaches.

2.5 Software Documentation

Software system documentation is very important because it preserve the history of the systems at different cycles and in turn facilitate the use of it by the users and maintainers. Basically, the objective of documentation is to teach, those unfamiliar with the system, how it is structured, how it works, and what the design motifs are. Additionally, software documentation facilitates interpretation of the system. Problem may arise and it will take time to solve if there is no specific guide. It's like going through a jungle without a map or compass. The result is significant loss of time and money many times. While software system documentation can be a tedious task, even more so when there are large scale, complex systems, someone has to do it. Documentation of maintenance systems must be done to run the system smoothly and it surly worth it in the long run.

2.6 Software Support and Maintenance

Software maintenance is one of the major concerns of software development and maintenance organizations. Software must be monitored constantly to ensure proper operation. Bugs and defects discovered in production must be reported and responded to, which often feeds work back into the process. Bug fixes may not flow through the entire cycle, however, at least an abbreviated process is necessary to ensure that the fix does not introduce other problems. During the Warranty Period, software vendor/ supplier/ developer shall provide to the executing agency any new, corrected or enhanced version of the software as created by developer. Such enhancement shall include:

- The client organization should maintain a register which must contain:
    1. i. Title and publisher of the software
    2. ii. Date and source of Software acquisition
    3. iii. Location of each installation
    4. iv. Software product's key number
- All modifications to the Software which increase the speed, efficiency or ease of use of the Software
- Add additional capabilities or functionality to the Software, but shall not include any substantially new or rewritten version of the Software
- An inventory of all software should be kept in the client organization, and give annual reports on status of utilization, support and adaptability.
- Executing agencies shall also determine which software have expired licenses for the purposes of upgrade or disposal. Where such systems have proprietary data, that data shall be extracted using suitable mechanisms.
- Software media and administration documentation, whether hardcopy or electronic, shall be securely stored in a central repository and copies may be created for backup and disaster recovery purposes as permitted by the license terms and conditions.
- Software maintenance shall be done in-house who shall develop a maintenance schedule on

upgrading and debugging. Sub-contracting for software maintenance shall be through appropriate justification and approval by the relevant Authority in the respective Executing agencies. Due diligence shall be undertaken in retaining such contractors.

- Software media shall be tagged with the standard government labeling conventions and appropriately physically secured.

2.7 Warranty of Functionality

For the period of warranty as specified in the contract following delivery of the software to the executing agency the software shall perform in all material respects according to the developer's specifications when used with the appropriate computer equipment. In the event of any breach or alleged breach of this warranty, the executing agency shall promptly notify the developer/ vendor and return the software to developer at executing agencies expense. Executing agencies sole remedy shall be that vendor/ developer shall correct the software so that it operates according to the warranty. This warranty shall not apply to the software if modified by anyone or if used improperly or on an operating environment not approved by the developer. After expiration of the warranty period licensee/ executing agency shall continue to receive maintenance support for a minimum of twelve month period or as agreed in in the contract. The charge for such maintenance support shall be developer's regular list price for maintenance and support for the software as published from time to time by developer.

2.8 End User License Agreement

The right to use the software must be acquired from the vendor under conditions defined within an end user license agreement. These terms and conditions vary considerably between vendors and individual software products. The guidelines and standard provides and prescribes best practices for software development, acquisition, support and maintenance by executing agencies. These best practices have been recognized to significantly contribute to the successful acquisition. Software guidelines and standards shall aim to assure software quality, ensure software internal usability, and help evaluate the software product. They are as follows-

- Executing agencies shall ensure that the software license agreements to do not prohibit data integration or movement of databases across different hardware platforms.
- All Computer software purchased shall include licenses for each user within the executing agency.
- A more cost effective license, such as site licenses, is recommended and executing agencies are responsible for purchasing licenses (through contracts, quotations, bids, or sole source) and furnishing their computer hardware vendors with proof of license or media;
- The computer hardware vendor will install the software on the server or clients as appropriate as part of their quoted hardware price;
- The vendor/supplier shall provide after sell training on the Software purchased/acquired for the IT personnel or any other designated officer within the executing agency;
- Clearly delegate and document responsibility and accountability for acquiring new software and records keeping of all items purchased;
- Acquire software only from reputable registered resellers;
- Safely store evidence of license documentation (original CDs/DVDs, Certificate of Authenticity, Retail Software License terms (also known as an End User License Agreement), original User's Manual, and sales receipt) in a centralized and safe location.
- Executing agencies shall track and update the software inventory on a regular basis to help ensure proper licensing and compliance.

2.9 Issues Associated with End User Agreement

Major software vendors do not generally sell directly; they instead utilize the services of a third party reseller. This relationship poses some challenges in purchasing as follows:

- While the purchase arrangement is with the reseller the actual contract usually exists between the organization and the vendor. This requires the organization to keep records in their purchasing and license management systems which accurately reflect this.
- The purchase of software from a reseller does not legally constitute license ownership of a software item. Ownership of the license does not exist until the vendor has issued the license. Typically this happens once the reseller has paid them for the software and the license is then issued in either hard copy or via an electronic license advice.
- Software purchases require entering into a legally binding contract with the vendor; the need to manage and review this contract can impact future purchasing.

2.10 Issues with Pre-Installed Software Installation:

The following guidelines shall be applied in acquisition of Non Pre-installed Software:

- Executing agencies shall verify that the End User License Agreement (EULAs) are provided by the Software vendor (s) to the reseller of supplier and with detailed Terms and Conditions under which the use of their software is permitted, information regarding the media associated with the license to allow for backup copies, copies to be archive for disaster recovery purposes or define other allowable methods of distribution.
- Executing agencies shall ensure that only licensed, registered and tracked software by the vendor shall be purchased or acquired for ease of upgrade, maintenance and proof of ownership.
- All executing agencies shall ensure that pre-installed software will have maintenance or upgrade options. This allows the license holder to use newer versions of the product as they become available over the time specified in the agreement. Proof of ownership of the original base license is required to be retained to support all future upgrades.
- Any pre-installed Software shall include support options by the vendor which must be carefully recorded to enable later use or renewal. The available options shall include but not limited to the following:
    - Ability to access updates and bug fixes
    - Manuals and other reference material
    - Workshops, pre-release seminars, training and
    - Technical Support, Help desk and other support facilities
- Different licensing options shall be required to be listed by the Vendor and should define how the Software can be deployed. Its therefore important that software licensing options are stated and shall fall within the following categories:
    - Site Licensing (to any user at a nominated site)
    - Enterprise Licensing (to all desktops within an organization) and;
    - Concurrent Licensing (which allows licenses to be allocated as required up to a maximum limit).

CHAPTER THREE
Hardware

3.1 Hardware

Computer hardware refers to the physical devices that make up a computer. Examples include the keyboard, monitor and disk drive. Hardware devices can be classified into four distinct categories:

- Input devices: For raw data input.
- Processing devices: To process raw data instructions into information.
- Output devices: To disseminate data and information.
- Storage devices*:* For data and information retention.

3.1.1 Input Device

Components which are used to input raw data are categorized under input devices. They aid in feeding data such as text, images, and audiovisual recordings. They even aid in file transfers between computers. The keyboard is probably the most commonly used input device. Below are just some other types of input devices.

Input Type	Examples
Pointing Device	Mouse, touchpad, touchscreen, multi-touch screen, pen input, motion sensor, graphics tablet, interactive smart board, and fingerprint scanner.
Game Controller	Joystick, gamepad, and steering wheel.
Audio Input Device	Microphone and midi keyboard.
Bluetooth Peripheral	Keyboard, mouse, headset, gamepad, printer.
Visual and Imaging Device	Webcam, digital camera, digital camcorder, TV capture card, biometric scanner, and barcode reader.
Network Device	Ethernet hardware and Bluetooth/wireless hardware.

3.1.2 Processing Device

Processing is the core function of a computer. It is the stage where raw data is transformed into information. Once data has been processed, it can be used for useful purposes. Components that manipulate data into information are categorized under processing. The microprocessor is the major device in this category. It works closely with primary memory during its operations. Data is stored temporarily in processor cache and primary memory during the processing period. The microprocessor is subdivided into three important units, which work together in order to accomplish its function. The units are:

i. The control unit: It manages and supervises the operations of the processor and other components that are crucial in data manipulation.

ii. Arithmetic and logic unit: The ALU is responsible for all arithmetic and logic operations like addition, multiplication, subtraction, division, and comparison logic operations.

iii. Register and cache: These are storage locations inside the processor that respond to the instructions of the control unit by moving relevant data around during processing.

3.1.3 Output Device

Hardware components that disseminate and display both data and information are classified under the output category. Output is the culmination of a cycle which starts with the input of raw data and processing. These components are sub-categorized under softcopy and hardcopy output. Softcopy output includes the intangible experience. The user derives visual satisfaction by reading a message through display components or listens to audio files through speakers. On the other hand, hardcopy output devices are tangible, like printouts of paper and 3D models.

3.1.4 Memory/ Storage Devices

Components that retain/ store data are classified under memory/ storage devices. Storage is sub-divided under primary and secondary memory and is either volatile or nonvolatile. Primary memory usually refers to random-access memory (RAM) but can also refer to all memory that works in tandem with the processor. RAM is volatile, meaning that it retains data only when the computer is powered up. The central processing unit (CPU) or accelerated processing unit (APU) reads instructions stored in this memory and executes them as required. Secondary memory is labeled as such because data stored within secondary storage media (usually disk drives) do not communicate directly with the microprocessor. Any data stored in such media is first transferred to a RAM device for processing to take place. This type of memory is also non-volatile since it permits long time storage as opposed to volatile memory. To give some examples of these devices, primary memory includes DRAM, SRAM and ROM whereas secondary memory is mainly subdivided into two categories:

i. Internal devices are designed to be placed inside the computer at all times. Examples include hard disk and solid state disk drives.

ii. External devices are plug and play media used to transfer files between computers. Examples include optical disks, flash disks, and external disk drives.

3.2 Minimum Hardware Specification

Must provide minimum specifications for commonly used, as a measure of ensuring standardization of equipment used across Government executing agencies. The following criteria shall be put into considering in developing minimum hardware specifications;

Interoperability: All hardware equipment shall exhibit the ability to run application programs from different vendors, and to interact with other IT hardware across local or wide-area networks regardless of their physical architecture and operating systems. This shall be feasible through hardware and software components that conform to open standards such as those used for internet; this seeks to facilitate the exchange of information between potentially heterogeneous systems through conformance to open standards.

Compatibility: All warranty repairs made to the system during the warranty period must maintain full compatibility of the system with installed software. Executing agencies shall ensure that the supplier lists a range of compatible devices or software that can be used together with the computer.

Upgradability: Executing agencies shall ensure that the IT hardware parts and related accessories are easily upgradable with new features to avoid IT products being disposed prematurely because some parts cannot be upgraded. Executing agencies shall in addition ensure that a list of all upgradable parts (including up to what capacity the parts can be upgradable) of the products supplied is provided by the supplier. IT component installations that need updates shall be updated according to the latest official versions available. This criterion provides the ability of IT equipment components to effectively and efficiently work together in an integrated system.

Total lifecycle: These specifications are meant to ensure that equipment acquired have useful life of not less than four (4) years.

Long-term support: This addresses the availability of vendor and/ or internal support, including parts and technical persons.

Scalability: This is intended to ensure that the acceptable IT components enhance the ability of the system to support future growth and increased throughput.

Availability: This seeks to maintain a system's operational readiness through robust and/ or redundant (e.g. fault tolerance) equipment.

Accessibility: This addresses operational readiness that includes the ability of users and operators to access the system in a timely fashion, to perform its intended functions.

Functionality: This intends to guarantee that operational requirements intended to be performed by IT systems, can be achieved effectively and efficiently with the equipment specified.

Security: This serves the need to protect system data and equipment, and the operational environment from loss or compromise. Each workstation connected to the Internet shall have a host antivirus and firewall active at all times.

Energy efficiency: Electronics play an increasingly large role in energy consumption. As a requirement therefore power usage of the IT hardware and other related accessories shall conform to Energy star an international standard for energy efficient consumer products. In addition all IT equipment supplied shall be expected to come with power Saving features or energy-saving models. Executing agencies are expected to verify with the supplier that the IT equipment are tested for electrical safety and test reports should form part of the documentations accompanying the products. All IT hardware products should be tested for electrical ssafety and test reports should form part of the documentations accompanying the computers.

3.3 Server

Server is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers. There are three considerations for purchasing servers

1. Server type: Tower, Rack or Blade
2. Hardware configuration
3. Server software

Tower Server

A tower server is a computer intended for use as a server and built in an upright cabinet that stands alone. The cabinet, called a tower, is similar in size and shape to the cabinet for a tower-style personal computer. This is in contrast to rack server s or blade server s, which are designed to be rack-mounted .

Rack Server

A rack server, also called a rack-mounted server, is a computer dedicated to use as a server. and designed to be installed in a framework called a rack. The rack contains multiple mounting slots called bays, each designed to hold a hardware unit secured in place with screws.

A single rack can contain multiple servers stacked one above the other, consolidating network resources and minimizing the required floor space. The rack server configuration also simplifies cabling among network components. In an equipment rack filled with servers, a special cooling system is necessary to prevent excessive heat buildup that would otherwise occur when many power-dissipating components are confined in a small space.

Blade Server

A blade server is a server chassis housing multiple thin, modular electronic circuit boards, known as server blades. Each blade is a server in its own right, often dedicated to a single application. Blade servers allow more processing power in less rack space, simplifying cabling and reducing power consumption.

Server Hardware Configuration

Servers use the same basic architecture or configuration. However, a server has enhanced hardware features such as

- Multiple multi-core processors
- Faster memory options for increased application performance
- Multiple hard drives for increased data capacity and redundancy
- Specialized networking cards

Mother Board/ System Board

As the backbone of a computer, the motherboard (sometimes called a system board or mainboard) connects all system components and allows them to interact. The motherboard also determines the major characteristics of a system, and affects choice of CPU, memory. and expansion capabilities.

Processor

The processor is the central brain of the server. The speed and number of processor in server has an enormous impact on server's ability to support applications. Processor is continuously changing and it can be difficult to determine the right one for the system.

i. **Clock speeds**

This is how fast the processor operates, usually measured in gigahertz (GHz). Servers with higher speed deliver better performance. This may enhance the ability to support more simultaneous outlook accounts, handle more web requests during peak demand periods and perform faster queries on customer database. Buying a higher frequency processor improves current system performance but also helps ensure server is able to handle future demand

ii. **Core count**

The number of physical processors within the processor itself. Today, most server CPUs have two or four cores. Multiple cores enable better multitasking on servers that will run multiple applications. For example, virus scans may run on one core while data backup is handled by another independent core.

iii. **Cache Size**

Each processor has built-in high speed memory located directly on and close to the central processing unit (CPU). Larger cache size reduces the frequency that the CPU needs to retrieve data from the system memory that sits outside of the CPU. For most applications, this improves the responsiveness of the system and provides a better user experience. Typically, CPUs with higher core counts and frequency have larger cache sizes to provide optimal performance.

Memory

When one open a file or document, server needs a place to temporarily keep track of that file. It uses high-speed specialized chips called random-access-memory, or RAM. The actual file is saved to hard drive once one 'save' the file. RAM is designed for fast access and quickly remembers where the file is stored in permanent hard drive system.

A general rule of thumb is the more RAM available, the more operations server can handle at the same time, without having to access the hard drives (which are slower than the RAM on the system board).

Storage or Hard Drive

Hard drives provide server with a large library of all the files it can access. Think of it like an ever-expandable file cabinet. The size and type of hard drive systems depends on just how much data one need to store.

Internal Storage

Most servers are configured with a very large hard. However, server hard drives are specially designed for fast access times and the ability to add multiple hard drives internally. Eventually, may need to add more hard drives and attach external hard drive systems.

RAID

Redundant Array of Independent Disks – combines hard drives into one large, logical storage system that writes data across more than one disk for greater reliability.

Network Controller

The network connection is one of the most important parts of any server. The network controller manages the inputs and traffic from the clients (other computers).

Power Supply

Because a server usually has more devices than a typical desktop computer, it requires a larger power supply (300 watts is typical). If the server houses a large number of hard drives, it may require an even larger power supply.

3.4 Procurement of Hardware

The following guiding principle shall be used in the procurement of IT hardware.

- Preference in the procurement of IT hardware and software shall be from an authorized dealer (licensed and accredited);
- Executing agencies shall ensure that the Bid and Contract document to supplier (s) include assigning a technical personnel (name and contact information) for addressing queries and support related with the use of the IT products supplied;
- In preparing the specifications for the procurement of IT Products (hardware and software) executing agencies shall ensure that installation, testing and commissioning of IT equipment

and software is included in the Bid and Contract document. In addition executing agencies shall ensure that these are done successfully prior to use of the IT equipment and software;

3.5 Registration and licensing of IT Product Suppliers

- The supplier(s) of IT equipment are registered and licensed locally by relevant designated Authority.
- That the suppliers (s) of specific brand of IT Products produce evidence or proof of certification and authorization by the manufacturer of a specific brand of IT Products.
- That the supplier provides proof of sourcing from the said manufacturer as per the manufacturers authorization provided before the IT products can be accepted by the procuring entity.

3.6 Documentation

Procuring agencies shall ensure that all IT hardware and software products are delivered with the following sets of documents in English; where in a different language the supplier shall ensure that the documents are accurately translated.

i. Certificate of origin
ii. Documents specifying Manufacture date and Model.
iii. Packing declaration document to enables executing agencies to check that the correct number of units has been received. Customs authorities can also easily identify a specific pack they wish to inspect.
iv. Evidence of testing, such as certificate of testing, proof of functional capability of item supplied.
v. Inspection certificates prior to shipment to Bangladesh.
vi. Import permit for certain IT Products (if required)
vii. Any components found to be malfunctioning must be replaced with an equivalent or its superior by the supplier/vendor(s).
viii. If a defect covered by warranty is discovered, that item must be repaired or replaced by the supplier or vendor on-site within the stated working days of notification by the procuring entity.

All IT equipment supplied or purchased from a vendor shall comply with the following issues-

- IT equipment purchased from a vendor should come with a set of documentation which allows the executing agency/ purchaser to operate and maintain the equipment. A complete document package may include the following:
- Test and inspection reports/records that allow the procuring entity to verify that the IT equipment has been supplied according to the quality and fabrication requirements of the specification, operating and maintenance manuals;
- IT equipment supplied or purchased with disconnected parts should be supplied with procedure guide for reassembling the parts.
- Certificate of Warranty for each of the IT hardware Product supplied at least (1 year parts only/or as per the agreed Contract).
- Instruction and Installation manuals for both software and Hardware products.
- Electrical Safety and Test reports should accompany the IT equipment being supplied

3.7 Emerging Technologies - Robotics and IoT

Emerging technology is a term generally used to describe a new technology, but it may also refer to the continuing development of an existing technology; The term commonly refers to technologies that are currently developing, or that are expected to be available within the next five to ten years, and is usually reserved for technologies that are creating, or are expected to create, significant social or economic effects.

1. Internet of Things (IOT)

The Internet of things is the network of devices such as vehicles, and home appliances that contain electronics, software, sensors, actuators, and connectivity which allows these things to connect, interact and exchange data.

The IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled.

2. Machine learning

Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it learn for themselves.

3. Virtual reality (VR)

Virtual reality (VR) is an interactive computer-generated experience taking place within a simulated environment. It incorporates mainly auditory and visual feedback, but may also allow other types of sensory feedback. This immersive environment can be similar

4. Touch commerce

Being able to buy anything with the touch of a finger may have seemed like a fantasy a few years ago, but it’s now a reality. Merging touchscreen technology with one-click shopping, touch commerce allows consumers to buy products easily from their phones. After linking their payment information to a general account and enabling the feature, customers are able to buy everything from clothes to furniture with just a fingerprint.

5. Cognitive Technology

Cognitive technology is in the same vein as machine learning and virtual reality except that it’s a broader concept. For example, the cognitive technology umbrella includes things like natural language processing (NLP) and speech recognition. Combined, these different technologies are able to automate and optimize a lot of tasks that were previously done by people, including certain aspects of accounting and analytics.

3.8 Characteristics of Non-compliant IT Equipment

Where IT equipment/products exhibit the following characteristics, it shall be considered non-compliant:

1. The product is not complete and some essential parts are missing;
2. Functionality or safety is impaired;
3. The appearance is generally worn or damaged;
4. It is destined for disposal or recycling instead of use; and
5. It is old or outdated destined to be cannibalized to gain spare parts.

CHAPTER FOUR
Networks

4.1 Network

A network is a collection of computers connected to each other. The network allows computers to communicate with each other and share resources and information. Computer networks can also be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as Optical fiber, Ethernet, Wireless LAN, Home PNA, or Power line communication. Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs, switches, bridges and/or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium.

4.2 Network Classification

The following list presents categories used for classifying networks. Based on their scale, networks can be classified as Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Personal Area Network (PAN), Virtual Private Network (VPN) etc. Computer networks may be classified according to the functional relationships which exist among the elements of the network, e.g., Active Networking, Client-server and Peer-to-peer (workgroup) architecture.

Computer networks may be classified according to the network topology upon which the network is based, such as Bus network, Star network, Ring network, Mesh network, Star-bus network, Tree or Hierarchical topology network, Network Topology signifies the way in which devices in the network see their logical relations to one another. The use of the term "logical" here is significant. That is, network topology is independent of the "physical" layout of the network. Even if networked computers are physically placed in a linear arrangement, if they are connected via a hub, the network has a Star topology, rather than a Bus Topology. In this regard the visual and operational characteristics of a network are distinct; the logical network topology is not necessarily the same as the physical layout.

4.3 Types of Networks

4.3.1 Personal Area Network (PAN)

A personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that are used in a PAN are printers, fax machines, telephones, PDAs and scanners. The reach of a PAN is typically about 20-30 feet (approximately 6-9 meters), but this is expected to increase with technology improvements. Personal area networks may be wired with computer buses such as USB and FireWire. A wireless personal area network (WPAN) can also be made possible with network technologies such as IrDA and Bluetooth.

4.3.2 Local Area Network (LAN)

This is a network covering a small geographic area, like a home, office, or building. Current LANs are most likely to be based on Ethernet technology. For example, a library may have a wired or wireless LAN for users to interconnect local devices (e.g., printers and servers) and to connect to the internet. On a wired LAN, PCs in the library are typically connected by category 5 (Cat5) cable, running through a system of interconnected devices and eventually connect to the Internet. The defining characteristics of LANs, in contrast to WANs (wide area networks), include their higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines.

4.3.3 Campus Area Network (CAN)

This is a network that connects two or more LANs but that is limited to a specific and contiguous geographical area such as a college campus, industrial complex, office building, or a military base. A CAN may be considered a type of MAN (metropolitan area network), but is generally limited to a smaller area than a typical MAN. This term is most often used to discuss the implementation of networks for a contiguous area. This should not be confused with a Controller Area Network. A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet.

4.3.4 Metropolitan Area Network (MAN)

A Metropolitan Area Network is a network that connects two or more Local Area Networks or Campus Area Networks together but does not extend beyond the boundaries of the immediate town/city. Routers, switches and hubs are connected to create a Metropolitan Area Network.

4.3.5 Wide Area Network (WAN)

A WAN is a data communications network that covers a relatively broad geographic area (i.e. one city to another and one country to another country) and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

4.3.6 Global Area Network (GAN)

Global Area networks (GAN) specifications are in development by several groups, and there is no common definition. In general, however, a GAN is a model for supporting mobile communications across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is "handing off" the user communications from one local coverage area to the next.

4.4 Internetwork

Two or more networks or network segments connected using devices that operate at layer 3 (the 'network' layer) of the OSI Basic Reference Model, such as a router. Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an internetwork.

In modern practice, the interconnected networks use the Internet Protocol. There are at least three variants of internetwork, depending on who administers and who participates in them:

- Intranet
- Extranet
- Internet

Intranets and extranets may or may not have connections to the Internet. If connected to the Internet, the intranet or extranet is normally protected from being accessed from the Internet without proper authorization. The Internet is not considered to be a part of the intranet or extranet, although it may serve as a portal for access to portions of an extranet.

4.4.1 Intranet

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

4.4.2 Extranet

An extranet is a network or internetwork that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities (e.g. a company's customers may be given access to some part of its intranet creating in this way an extranet, while at the same time the customers may not be considered 'trusted' from a security standpoint). Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

4.4.3 Internet

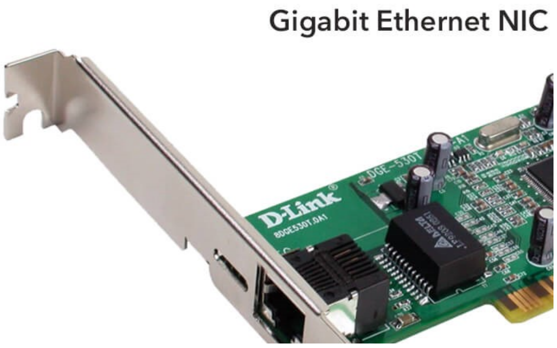
The Internet is a specific internetwork. It consists of a worldwide interconnection of governmental, academic, public, and private networks based upon the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the U.S. Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).

4.5 Basic Components for networks

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required, usually in the form of galvanic cable (most commonly Category 5 cable). Less common are microwave links (as in IEEE 802.11) or optical cable ("optical fiber").

i. Network Interface Cards

A **network card**, **network adapter** or **NIC** (network interface card) is a piece of computer hardware designed to allow computers to communicate over a **computer network**. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.



ii. Repeaters

A **repeater** is an electronic device that receives a signal and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair ethernet configurations, repeaters are required for cable runs longer than 100 meters away from the computer.

iii. Hubs

A hub contains multiple ports. When a packet arrives at one port, it is copied to all the ports of the hub for transmission. When the packets are copied, the destination address in the frame does not change to a broadcast address. It does this in a rudimentary way: It simply copies the data to all of the Nodes connected to the hub.

iv. Bridges

A **network bridge** connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

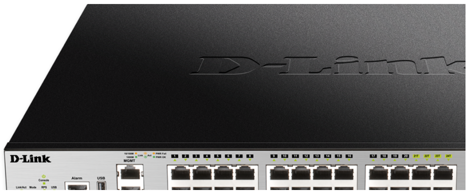
Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Bridges come in three basic types:

1. Local bridges: Directly connect local area networks (LANs)
2. Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced by routers.
3. Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

v. Switches

A switch is a device that performs switching. Specifically, it forwards and filters OSI layer 2 datagrams (chunk of data communication) between ports (connected cables) based on the MAC addresses in the packets. This is distinct from a hub in that it only forwards the datagrams to the ports involved in the communications rather than all ports connected. Strictly speaking, a switch is not capable of routing traffic based on IP address (layer 3) which is necessary for communicating between network segments or within a large or complex LAN. Some switches are capable of routing based on IP addresses but are still called switches as a marketing term. A switch normally has numerous ports, with the intention being that most or all of the network is connected directly to the switch, or another switch that is in turn connected to a switch. Switch is a marketing term that encompasses routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier). A device that operates simultaneously at more than one of these layers is called a multilayer switch.



vi. Routers

Router**s** are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. Routers work at the network layer of the TCP/IP model or layer 3 of the OSI model. Routers also provide interconnectivity between like and unlike media (RFC 1812). This is accomplished by examining the Header of a data packet, and making a decision on the next hop to which it should be sent (RFC 1812) They use preconfigured static routes, status of their hardware interfaces, and routing protocols to select the best route between any two subnets. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Some DSL and cable modems, for home (and even office) use, have been integrated with routers to allow multiple home/office computers to access the Internet through the same connection.

vii. Client Server

The **client-server** architecture model distinguishes client systems from server systems, which communicate over a computer network. A client-server application is a distributed system comprising both client and server software. A client software process may initiate a communication session, while the server waits for requests from any client. Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server. Standard networked functions such as email exchange, web access and database access, are based on the client/server model. For example, a web browser is a client program at the user computer that may access information at any web server in the world.

To check bank account from a computer, a web browser client program in a computer forwards the request to a web server program at the bank. That program may in turn forward the request to its own database client program that sends a request to a database server at another bank computer to retrieve the account balance. The balance is returned to the bank database client, which in turn serves it back to the web browser client in the personal computer, which displays the information. The client/server model has become one of the central ideas of network computing. Most applications being written today use the client/server model. So do the Internet's main application protocols, such as HTTP, SMTP, Telnet, DNS, etc. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the "monolithic" centralized computing of mainframe computers. But this distinction has largely disappeared as mainframes and their applications have also turned to the client/server model and become part of network computing. Each instance of the client software can send data requests to one or more connected *server*s. In turn, the servers can accept these requests, process them, and return the requested information to the client. Although this concept can be applied for a variety of reasons to many different kinds of applications, the architecture remains fundamentally the same.

The most basic type of client-server architecture employs only two types of hosts: clients and servers. This type of architecture is sometimes referred to as *two-tier*. It allows devices to share files and resources. The two tier architecture means that the client acts as one tier and application in combination with server acts as another tier. These days, clients are most often web browsers, although that has not always been the case. Servers typically include web servers, database servers and mail servers. Online gaming is usually client-server too. In the specific case of MMORPG, the servers are typically operated by the company selling the game; for other games one of the players will act as the host by setting his game in server mode.

The interaction between client and server is often described using sequence diagrams. Sequence diagrams are standardized in the Unified Modeling Language. When both the client- and server-software are running on the same computer, this is called a single seat setup.

Characteristics of a Client

- Initiates requests
- Waits for replies

- Receives replies
- Usually connects to a small number of servers at one time
- Typically interacts directly with end-users using a graphical user interface

Characteristics of a Server

- Never initiates requests or activities
- Waits for and replies to requests from connected clients
- A server can remotely install/uninstall applications and transfer data to the intended clients

4.6 Cloud Computing

Cloud computing is a type of computing that relies on shared computing resources rather than having local servers or personal devices to handle applications. In its most simple description, cloud computing is taking services (″cloud services″) and moving them outside an organization's firewall. Applications, storage and other services are accessed via the Web. The services are delivered and used over the Internet and are paid for by the cloud customer on an as-needed or pay-per-use model.

4.6.1. Software as a Service (SaaS)

SaaS is a software delivery method that provides access to software and its functions remotely as a Web-based service. Instead of paying an upfront fee to purchase and/or license software, SaaS customers pay a recurring (often monthly or annual) fee to subscribe to the service. In general, they can access the SaaS from any Internet-connected device, any time day or night. Well-known examples of SaaS include Salesforce.com, Microsoft Office 365, Google G Suite, Dropbox, Adobe Creative Cloud and others.

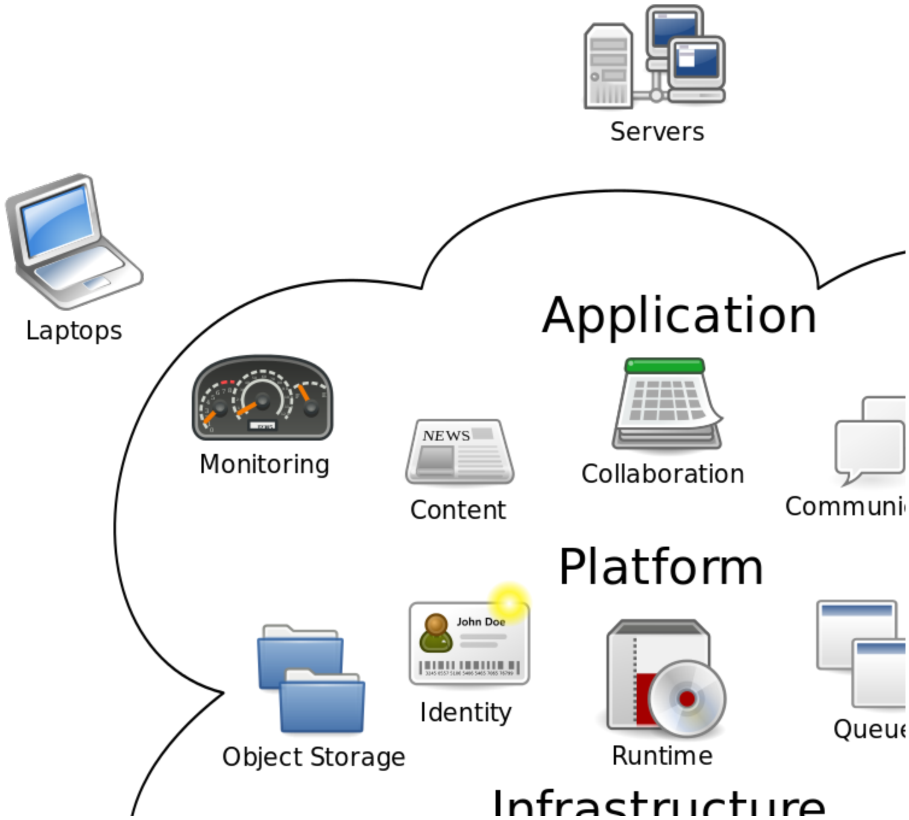
4.6.2. Platform as a Service (PaaS)

PaaS is a computing platform being delivered as a service. Here the platform is outsourced in place of a company or data center purchasing and managing its own hardware and software layers. Most PaaSes are designed for developers and aim to simplify the process of creating and deploying software. For example, a Web developer might use a PaaS that includes operating system software, Web server software, a database and related Web development tools. The leading PaaS vendors include Amazon Web Services, Microsoft Azure, IBM and Google Cloud Platform.

4.6.3 Infrastructure as a Service (IaaS)

Computer infrastructure, such as servers, storage and networking delivered as a service. IaaS is popular with enterprises that appreciate the convenience of having the cloud vendor manage their IT infrastructure. They also sometimes see cost savings as a result of paying only for the computing resources they use. The leading IaaS vendors include Amazon Web Services, Microsoft Azure, IBM and Google Cloud Platform.

While SaaS, PaaS and IaaS are the three most common types of cloud services, cloud computing vendors sometimes also use other "as a service" labels to describe their offerings. For example, some offer database as a service (DBaaS), mobile back-end as a service (MBaaS), functions as a service (FaaS) or others.



4.7 Characteristics of Cloud Environments

All cloud environments have five key characteristics:

i. **On-demand self-service:** This means that cloud customers can sign up for, pay for and start using cloud resources very quickly on their own without help from a sales agent.

ii. **Broad network access:** Customers access cloud services via the Internet.

iii. **Resource pooling:** Many different customers (individuals, organizations or different departments within an organization) all use the same servers, storage or other computing resources.

iv. **Rapid elasticity or expansion:** Cloud customers can easily scale their use of resources up or down as their needs change.

v. **Measured service:** Customers pay for the amount of resources they use in a given period of time rather than paying for hardware or software upfront. (Note that in a private cloud, this measured service usually involves some form of chargebacks where IT keeps track of how many resources different departments within an organization are using.)

CHAPTER FIVE
Security

5.1 Physical and Environmental Security

Physical and Environmental security aims at protecting executing agencies ICT facilities like hardware, software, data and communication infrastructure from unauthorized access, hazards, intentional or unintentional damage, as well as theft. Breach of physical and environmental security may lead to loss of confidentiality, integrity, and availability of information systems assets. To prevent such loss, measures such as adequate air conditioning, fire detection and suppression systems, reliable power supplies, controlling physical access and suitable emergency preparedness should be in place. The envisaged measures are as follows:

5.1.1 Measures against Fire

i. Rooms that host servers should be non-smoking zones, fireproof, fitted with smoke detectors and have automatic or portable fire extinguisher systems.
ii. Smoke detectors and fire extinguishers should be regularly tested to ensure that they are in good order and all tests have to be documented.
iii. Materials which can easily catch fire should be disposed of and those documents which are still in use should be stored in a secure place.
iv. Activities such as rewiring, welding or cutting, undertaken as part of structural changes to the premises, should be monitored by ICT staff, so long as there is proof of safety of new wiring required.
v. Clear fire instructions should be available and in the event of fire, these instructions should be followed.
vi. Regular fire practices (fire drills) should be conducted frequently.

5.1.2 Measures against Floods/Overflow of water

i. Servers should be well mounted on racks and other equipment should be kept off the ground, placed on tables or desks.
ii. Clear flood instructions should be available and in the event of flood, these instructions should be followed.
iii. All water tanks and plumbing at premises should be inspected regularly to prevent leaks and overflow of water. All inspection reports should be well kept for future reference.

5.1.3 Air Conditioning

i. The Server rooms and computer rooms should be adequately air conditioned to provide conducive environment for the ICT equipment.
ii. The air conditioners should be serviced regularly to ensure continuous performance.
iii. Air conditioning failure should be reported for immediate remedial measures.

5.1.4 Power Outage

To ensure ICT services availability, alternative power sources such as Uninterruptible Power Supplies (UPS) and generators should be used to provide continuous power supply based on the following requirements:

i. UPS should be installed as appropriate to all ICT facilities.
ii. Specialized UPS of appropriate capacity should be installed in all server rooms.
iii. Non-critical electrical equipment, especially high power consumption equipment such as photocopiers, printers and kettles should not be connected to UPS sockets.

iv. A generator of appropriate capacity should be serviceable at all times as backup power supply in the event of power outage.

5.1.5 Measures against Theft

i. Internal movement of ICT equipment owned by agencies should be authorized by the relevant authority in written form. Proper record should be kept for such movements.
ii. Moving ICT equipment owned/leased by Executing agencies outside the premises should follow laid down procedures.
iii. Appropriate locks on windows and doors should be maintained. Doors should be kept locked when rooms are not in use. Secure system for keys and combinations should be maintained. In the event of security breach, compromised lock should be changed.
iv. Alternative physical security strategies should be used when appropriate.
v. All legitimate visitors should be logged at the entrance to Executing agencies building and must declare ICT equipment.
vi. All staff must declare personal ICT equipment at the entrance.

5.2 Access control

Access control includes measures that need to be taken to control user access to computing areas and their associated systems. This is categorized into two areas namely physical access and logical access.

5.2.1 Physical Access Control

Both Server and Computer rooms should be protected against unauthorized access. The authorization of access to Computer and Server Rooms, and Disaster Recovery Site should base on the following requirements:

i. Normal hours of entry for the Computer and Server Rooms will be limited to approve times.
ii. Staff/Visitors authorized to enter the Server and Computer rooms should be accompanied by designated officer. Visitors should be logged in the register book.
iii. All staff should be trained on how to observe access procedures.
iv. Visitors should display visitors pass at all times.
v. ID cards and keys should not be shared or exchanged.
vi. All staff who have their access rights withdrawn should return the ID cards to Permanent Secretary-Treasury/Executing agencies.

5.2.2 Logical Access Control

5.2.2.1 Managing User Profiles

Access to the Computer systems should be authorized by the relevant authority, or appropriate delegated officer. Access to any particular data file should be based on the user's roles as established by his or her official duties, and should be reflected in the provision of specific authorization codes, passwords or other access-enabling means.

i. Users should be issued Unique User IDs that are produced following a standard naming convention.
ii. Before being granted logical access, users should complete a "User Access Permission Application Form" that defines access privileges. The user permission application form is attached.
iii. Users should be granted access and privileges based on their roles.
iv. Changes to Access Rights should only be made under authorization of the relevant authority.

v. Designated Systems administrator should review and maintain User Access Profiles.

vi. Privileges should be allocated to network and/or application software accounts on an 'as needs' basis. i.e. no more access should be offered than is necessary to carry out the user's needs.

vii. User account names should not indicate their associated privileges.

viii. The default password for an account should be constructed in accordance with systems password policy.

ix. Working groups or teams should be assigned their own access profile with specific network resource access. Individual users allocated to such groups should be given an account linked to that access profile.

5.2.2.2 Managing Network Access Controls

i. Access to resources on the systems network should be restricted unless specifically authorized.

ii. Users are expressly forbidden from making unauthorized alterations or extensions to the network.

iii. A register of network devices, their access restrictions and the protocols in use should be kept by the Network Administrator.

iv. All changes to network configurations should be recorded in the register, along with authorization for the changes.

v. Users should be permitted to use only those network addresses issued to them by the relevant authority.

vi. Virtual networks should be set up for specific groups of users. These groups should have Group User Access Profiles, on which the user access profiles of individual team members should be based.

vii. Users inside executing agencies network should not be allowed to use devices which connect to external networks, for example, the use of modem to connect to the internet.

viii. Remote users should connect to servers using a secure communication channel such as Virtual Private Network on dedicated communications lines with end-to-end encryption.

ix. Network devices and traffic should be monitored regularly.

x. Results/Logs from the firewall should be reviewed by ICT security officer to confirm there have been no unexpected attempts to connect.

xi. Users should not extend or re-transmit network services and traffic in any way i.e. they should not install a router, switch, hub, or wireless access point to the systems network without being approved.

xii. Users should not install network hardware or software that provides network services without being approved.

xiii. Computers that require network connectivity should conform to systems standards.

xiv. Users with administrative privilege should not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, system users should not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the system network infrastructure.

xv. Users are not permitted to alter network hardware in any way.

5.2.2.3 Controlling Administrative Access or Special Access

Employees with administrative access or special access privileges to the system are subject to additional controls for creation, use, monitoring and removal of their user access profiles. All users of administrative or special access accounts are given account management instructions, documentation, training, and authorization and should meet the Systems Password Policy.

5.2.2.4 Passwords Management

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords should not be shared with any other person for any reason.

i. Passwords should be chosen by the user not by the systems administrator. Where this is not practical, the password should be generated and the user should be forced to change the password at first logon.
ii. Users should sign “User Access Permission Application Form” that a password has been received, that it will be kept secret, and changed frequently.
iii. Disclosure of passwords is prohibited.
iv. Paper based records of passwords of systems super user should be placed in a sealed envelope, signed by two authorized persons across the seal, and keep it in a locked, fireproof safe.
v. Passwords should be changed the moment that a breach of confidentiality is suspected.

5.2.2.5 Controlling Remote User Access

Remote access control procedures should provide adequate safeguards through robust identification, authentication and encryption techniques based on the following requirements.

i. If an authorized user fails to gain access through the secure communication channel such as VPN, this should be immediately reported to the ICT unit for investigation.
ii. Remote User accessing Executing agencies systems should be authenticated by remote access server.

5.2.2.6 Clear Screen

All users of workstations, PCs and laptops with access to system, or containing related files, should ensure that their screens are clear of data when not in use. Moreover, user computers should be set so that they automatically switch to a standby mode after a period of inactivity. A password should be needed to regain access to the screen.

5.2.2.7 Logon and Logoff from Computer

To avoid Information security breaches, users should lock or log off their computers while they are not in use. If a user is unable to log on, it might indicate that someone has achieved unauthorized access using that user’s name and password. Where the 'User Logon Register' or operator/administrator logs show incorrect or unusual entries, it could indicate that data has been accessed and therefore possibly lost or stolen. The following requirements should be adhered to:

i. Every user should ensure that their user name and password are kept secret.
ii. If users are unable to logon to the system and denied service, they should double-check that the user name and password are correct and ensure that they are not still logged on elsewhere on the system.
iii. If users are still unable to log on, they should immediately inform their systems administrator. They should not ask to ‘borrow’ the user name and password of another user in order to log on.
iv. Users should ensure that they log off and shut down, if they expect to be away from their desk or work area for a prolonged period and at the end of the working day before they leave office premises.

v. Designated Systems Administrator should monitor the 'User Logon Register' or operator/administrator logs for unusual entries.
vi. Designated Systems Administrator should disable any suspicious logon.
vii. Designated Systems Administrator should report inability of users to log on to the designated Information Security Officer.
viii. Designated Systems Administrator should double check that users have logged off at the end of the working day.
ix. Users should ensure that they log off computer workstation before leaving their desk.

5.3 Data and Information Security

Data security is a critical responsibility for every institution. Every piece of data can be of value to fraudsters as they can access multiple sources of information and aggregate it. It is therefore, necessary that, executing agencies data and information is protected from unauthorized access, loss, misuse, destruction and falsification.

5.3.1 Data Collection, Entry and Processing

All processes of data collection, data entry and processing should be done in such a way that the records collected and captured are correct and complete. Data captured should then be validated for accuracy by relevant departments/units.

5.3.1.1 Data Storage

i. All users of information systems should save their work on the system regularly.
ii. When information and data is stored on local disks (e.g. notebook computers), they should be backed up to the server regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

5.3.1.2 Data Access

i. Authentication and authorization functions should be used for all users of executing agencies electronic data and information resources.
ii. Procedures to manage access, authentication and authorization should be developed to support and manage these activities. Such processes and procedures should include but not limited to user passwords for network and application access, biometric access mechanism, tokens and electronic key devices.
iii. All system users should be created in a central authentication database.

5.3.2 Transfer and Exchange of Information

Data or information may only be transferred across networks or copied to other media when the confidentiality and integrity of the data is reasonably assured. The security mechanisms should reflect the sensitivity of the information involved and the following security conditions should be observed.

i. Information classified as confidential or secret should be encrypted.
ii. Private encryption keys should be physically exchanged rather than transferred electronically.
iii. Management responsibilities for controlling and notifying transmission dispatch and receipt.
iv. Minimum technical standards for packaging and transmission.
v. Use of reliable and trusted courier for data transportation/transfer.
vi. Responsibilities and liabilities in the event of loss of data.
vii. Use of an agreed labeling system for critical information.

viii. Technical standards for recording and reading information and software.

5.3.3 Security of Media in Transit

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. Thus, it is important to safeguard computer media being transported between sites based on the following requirements:

i. Reliable and trusted transport or couriers should be used.
ii. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
iii. Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e.g. by use of locked containers, delivery by hand, or use of tamper-evident packaging.

5.3.4 Data Retention and Disposal

i. Executing agencies should ensure that information is retained for appropriate time frame depending on requirements as in Records & Archives Management.
ii. All data to be disposed off should be erased permanently from any storage media. Data storage media should be verified that data is erased and cannot be read before disposing them as stipulated in Records & Archives Management.

5.3.5 Using Live Data for Testing

The use of live data for testing new systems or system changes is only permitted where adequate controls for the security of the data are in place. Using live data for testing can severely compromise its integrity and confidentiality and should base on the following requirements:

i. Where contracted suppliers and other third party staff are involved, a non-disclosure agreement should be signed, together with a declaration of compliance with executing agency.
ii. Designated system developers should not be permitted to access the live system and its database.
iii. Safe and secure copy of the data should be provided, once the terms of use have been authorized.
iv. Development and testing work should be isolated from normal processing work by means of separate machines or partitions.
v. The techniques used to capture the live data should not permit subsequent or additional access to the live system by the Designated System Developers.
vi. Output from testing should be differentiated from live output (e.g. by different colored paper or overprinting the words 'Test Data'). All test output should be kept within the test room/area.
vii. Test files that contain copies of live data should be disposed of after use. Test printouts containing live data should be destroyed after use.

5.4 Network, Internet and e-Mail Security

With networked or distributed applications, the security of multiple systems as well as the security of the interconnecting network, internet and its services is important, especially when public access wide area networks are used. This is due to the fact that while internet is increasingly becoming a standard working tool for organizations, criminals may target system via the internet. This could result in serious loss of confidential information or serious damage to information systems, such as premeditated virus attacks. To protect against premeditated or opportunistic attacks, security on the network is to be maintained at the highest level consistent with user needs.

5.4.1 Network Security

The designated executing agencies network administrator should ensure the security of information in networks and protection of supporting infrastructure based on the following requirements:

i. Keep network secured by minimizing number of network interface points between “secured” network and “non-secured” network.
ii. Keep network secured by separating internal networks and external networks.
iii. Executing agencies networks should not be extended to other external networks without permission.
iv. Only allow authorized traffic to enter the “secured” network.
v. Use multiple mechanisms to authenticate user (e.g. password system plus preregistered IP/IPX network plus pre-registered MAC address/terminal number).
vi. Manage the network with network management system.
vii. Encrypt data with approved encryption algorithm before transmitting over the network.
viii. Firewall, and intrusion prevention and detection system should be installed and properly configure to protect Executing agencies network.
ix. All access points of the network layout should be identified, and checks carried out to verify that safeguards are operational.

5.4.2 Wireless Network Security

Wireless Network is a type of network that uses high-frequency radio waves. With the advancement of technology and advances in price/performance, wireless accessibility is becoming increasingly deployed in the office or in public places. Security controls should base on following requirements:

5.4.2.1 Management Controls

i. Wireless network should be used with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.
ii. Designated System Administrator should develop a coverage map of the wireless network, including locations of respective access points and Service Set Identifier (SSID) information so as to avoid excessive coverage by the wireless signal.
iii. Designated System Administrator should regularly search for rogue or unauthorized wireless access points;
iv. Once a device is reported missing, Designated System Administrator should modify the encryption keys and SSID.

5.4.2.2 Network Design and Technical Controls

The Designated System Administrator should ensure the following:

i. Change product default access point configuration settings.
ii. Disable all insecure and unused management protocols on access points.
iii. Enable and configure security settings to make sure that unauthorized users do not gain access to Executing agencies wireless network.
iv. Ensure all wireless connections are connected to the security equipment (e.g. firewall, router).
v. Activate logging features and redirect all log entries to a logging server. The log records should be checked regularly.
vi. Deploy secure wireless technologies on top of wireless network.

vii. Segment the access point's coverage areas to balance the loading to minimize the probability of Denial-of-Service (DoS) attack.

5.4.2.3 Client Controls

The Designated System Administrator should:

i. Activate personal firewall on wireless clients (e.g. laptops, PDAs) that are used outside Network boundary.
ii. Turn off sharing at wireless clients.
iii. Keep strict control of the wireless interface cards (e.g. PCMCIA card for laptop) as access credentials such as SSID and/or encryption key are commonly stored on the card.
iv. Enable wireless connections only when users need them and disable them when they are no longer in use.
v. Follow the guideline protection against computer virus and malicious code.

5.4.3 Internet Security

Executing agencies should strike a balance between taking advantage of the Internet and maintaining security and confidentiality based on the following requirements:

i. Browsing of Internet sites containing pornographic, obscene, and immoral or any other inappropriate content is prohibited.
ii. ICT unit should ensure that Executing agencies network is protected from harm and danger that come with the use of the internet.
iii. Executing agencies internet service/connection should not be used to perform illegal acts and unauthorized activities.
iv. The ICT unit should strive to maintain a fast, efficient and secure internet connection. To maintain such quality, services such as media streaming and downloading, social network sites and online games are discouraged during working hours.
v. All access to the internet should be routed through web filtering hardware and monitoring software.
vi. All temporary staff and visitors are bound to this guideline.

5.4.4 E-mail Security

E-mail communication is very efficient and cost effective at communicating in written and multimedia form. E-mails can reach global masses in an instant. It is this ease of use that makes email communication open to abuse. In addition, email communication has the potential to advance illegal and unlawful course, as well as transmit harmful content such as computer viruses. It is for this reason that measures must be put in place to ensure that email communication is used responsibly based on the following requirements:

i. Users should use e-mail responsibly and preferably for official matters.
ii. Users should not open or forward any e-mail from unknown or suspicious sources.
iii. Users should not copy or forward chain e-mails. Chain emails can disrupt email services and other internet services on Executing agencies network.
iv. If users suspect or discover e-mail containing computer viruses or phishing attacks, they should report the incident to the designated Information Security Officer.
v. The e-mail system should not be used to commit unlawful and illicit acts.
vi. The users should avoid publishing e-mail address to unknown individuals or exposure of users' credentials by filling forms from dubious links and websites.

vii. Users should use separate e-mail addresses different from their office e-mail addresses when participating in public newsgroup or chat rooms, to avoid their office e-mail addresses and/or mail systems to become a target of spam.
viii. Users should not reply to spam because most return addresses are not legitimate and would only result in the generation of non-delivery messages thus increasing the amount of undesired traffic.
ix. Users should control spam by using e-mail filtering tools in e-mail software that allow users to block or screen out spam by defining some simple filtering rules.
x. User should not send e-mails using another person's e-mail account.
xi. Only encryption authorized by the Executing agencies should be used to encrypt e-mails.
xii. Mail systems should have a mechanism to scan e-mail attachment for viruses and other malicious before sending or downloading.

5.4.5 Protection against Cyber Attacks

In addition to network, internet and e-mail protections the following guidelines should be adhered to in order to protect against cyber-attacks:

i. Pattern analysis should be used to identify changes in on-line activity that may indicate a cyber-attack.
ii. ISP and designated systems administrator should ensure that the following categories of data are retained:
    a. Data necessary to trace and identify the source of a communication.
    b. Data necessary to identify the destination of a communication.
    c. Data necessary to identify the date, time and duration of a communication.
    d. Data necessary to identify the type of communication.
    e. Data necessary to identify users' communication equipment.
    f. Data necessary to identify the location of mobile communication equipment.

5.4.6 Protection against Computer Viruses and Malicious Code

Potential damages may include modifying data, destroying data, stealing data, allowing unauthorized access to the system and popping up unwanted screens. Protection against Computer viruses and malicious code should be done based on the following requirements:

i. Designated Executing agencies System Administrator should enable real-time detection to scan computer virus and malicious code for active processes, executables and document files that are being processed.
ii. Designated Executing agencies System Administrator should scan any files on electronic or optical media, and files received over networks against computer virus and malicious codes before use.
iii. Designated Executing agencies System Administrator should make sure e-mail server is configured such that attachments and downloads are automatically scanned against computer virus and malicious code before use.
iv. Before installing any software, Designated Executing agencies System Administrator should verify its integrity (e.g. comparing checksum value) and ensure it is free from computer virus and malicious code.
v. Installation of any software or file received via e-mail or downloaded from web browsing should be approved by Executing agencies relevant authority.
vi. Users should always boot from the primary hard disk. Booting workstations from removable storage device should not be done without permission.

vii. Designated Executing agencies System Administrator should conduct daily update of the virus definition files to minimize the risk of infection from new viruses.
viii. Designated Information Security Officer should prepare and implement user's awareness training programs on virus issues.

5.4.7 Responding to Virus Incidents

i. The Designated Information Security Officer should take all relevant details from the caller about the nature of the virus, its possible origins, and any previous alerts.
ii. The Designated Information Security Officer(s) should scan the relevant file(s) with antivirus software, to determine whether the virus has been immunized.
iii. The Designated Information Security Officer should establish whether the virus may have infected others and, if so, respond accordingly; if necessary by closing down workstations and even parts of the network.
iv. Users should communicate details to the designated Information Security Officer, seeking any additional guidance as necessary.
v. The Designated Information Security Officer should communicate new virus alert to warn personnel about the incident and the appropriate response.
vi. The Virus Incident Response Procedures will be documented if a virus (or other malicious code) affects Executing agencies critical systems.
vii. Ability to respond to virus incidents should be regularly reviewed and tested. Failure to respond appropriately to a virus incident can rapidly result in multiple systems failures and continued infection.

5.4.8 Protecting Against Internal Attacks (Insider Threats)

In order to reduce the incidence and possibility of internal attacks, access control and data classification policies and procedures are to be maintained at all times and periodically reviewed based on the following requirements:

i. Enforce separation of duties and least privilege on the system.
ii. Log, monitor and audit employee actions on the system.
iii. Conduct periodic security awareness training to all employees.

5.5 Software Security Management

Information systems used at Executing agencies shall either be developed internally or acquired as per Executing agencies requirements. Organizational security may be compromised if software development or acquisition will not consider security issues. All software development, acquisitions, deployment and usage at Executing agencies should be coordinated centrally by ICT Unit to ensure conformity to predefined standards. The following are measures that are to be considered in software security management:

Software Development

Security features should be considered by all executing agencies for software development. These features include:

i. Segregation of duties.
ii. Proper authentication and authorization.
iii. Proper session management.
iv. Input validation.
v. Data authenticity and integrity.
vi. Software should be tested so that the logical errors are rectified accordingly.

5.5.1 Software Acquisition

i. On acquiring software, proper procurement procedures should be followed as stated in the Public Procurement Act and its Regulations.
ii. All software acquired by Executing agencies should have documentation manuals and bear legitimate licenses.
iii. Usage of primary and secondary license should not be interchangeable.
iv. Delivery and guaranteed of functionality of acquired software should be the responsibility of the supplier.
v. Executing agencies ICT Unit should ensure proper management of licenses for the software acquired.
vi. Acquired critical software should be covered by escrow agreement to ensure continuity.

5.5.2 Software Deployment

Software deployment involves the installation and testing of software.

i. Testing of the software to be deployed should be conducted sufficiently such that security is not compromised.
ii. The ICT staff should prepare a well-documented test plan before software installation. The plan should be approved by the supervisor.
iii. Installation and activation of software should follow manufacturer's security standard, provided that they comply with Executing agencies security standards.
iv. All software to be deployed at Executing agencies should be free from virus or malicious code.
v. Installation should be done properly. Any deployment of software in Executing agencies environment should be approved by relevant authority.
vi. All software customizations should comply with user department requirements and Executing agencies security guidelines.
vii. Designated officer should verify that need for a particular customization has been met.

5.5.3 Software Usage

i. Software should be used for intended purpose as stipulated in terms and conditions of the software.
ii. Before an employee is permitted to use a particular software, the designated department should instruct users on the proper usage of the particular program.
iii. Designated department should inform users on terms and conditions included in the license agreement accompanied by the program.

5.5.4 Systems Integration and Interoperability

i. In order to ensure confidentiality, integrity and availability of data and information, all Executing agencies information systems should be integrated.
ii. Any new system should be compatible and interoperable with existing system without compromising organizational security.
iii. Different existing systems should be integrated by adhering to ICT security standards.

5.5.5 Software Change Management

Software Change Management is the process of planning, organizing, controlling, executing and monitoring changes that affect the delivery of ICT services. It encompasses all components and activities required to direct additions, modifications and deletions.

5.5.5.1 Implementing New or Upgraded Software

The implementation of new or upgraded software must be carefully planned and managed as a project for critical systems. Security risks will be minimized basing on the following requirements:

i. All staff involved in installing the new software or upgrade should be suitably qualified, trained or supervised.
ii. A suitable contingency plan should be in place in case of failure of the new software.
iii. Systems Administrator should properly test new or upgraded software before using in a live environment based on approved pre-designed test plan.
iv. Upgraded software versions should offer at least the current level of security safeguards.
v. System owner should decide the specific criteria and cut-off date, which will trigger a reversion.
vi. Regression Testing should test all the key features of the software not just those which have been changed or updated.
vii. System owner should always ensure that an upgraded software version can read and write files in the older format.
viii. Major upgrades of operating system version on the Executing agencies servers should be avoided unless there is a genuine reason for the upgrade.

5.5.5.2 Applying Patches/Service Packs

If a patch is applied incorrectly or without adequate testing, the system and its associated information can be placed at risk, possibly corrupting live data files. Patches applied to resolve software bugs shall only be applied when verified as necessary and with authorization from the user department based on the following requirements:

i. Patches should be from a reliable source and are to be thoroughly tested by the system administrator before use.
ii. System administrator should verify that the patches are necessary and come from an authorized source, normally the software manufacturer or vendors.
iii. System administrator should ensure that updates to the system documentation are received with the patches.

5.5.5.3 Responding to Vendor Recommended Upgrades to Software

The decision whether to upgrade Executing agencies's software is to be taken only after consideration on the associated risks and costs of the upgrade against the anticipated benefits and necessity for upgrade. Vendors' proposals for upgrade of operating systems or application programs should be appraised taking the following into account:

i. The upgrade is in line with overall strategy for Executing agencies system development.
ii. The vendor's motives for recommending the upgrade are ascertained.
iii. Contract should stipulate vendors' role on supporting (old) version.

5.5.5.4 Capacity Planning and Testing

Capacity Planning is the determination of the overall size, performance and resilience of a system. New and upgraded software must be planned and tested for expected future capacity and subjected to stress testing based on the following requirements:

i. It should demonstrate a level of performance and resilience which meets or exceeds the technical and requirements of Executing agencies systems.
ii. New and upgraded software should be subjected to transaction volumes that simulate or exceed expected future live requirements.
iii. Any areas where system testing has not been representative of the live environment should be identified, and the resultant risks evaluated.

5.5.5.5 Parallel Running

Parallel Running is the process of running a new or amended system simultaneously with the old system to confirm that it is functioning properly before use. This process should base on the following requirements:

i. Normal system testing procedures should incorporate a period of parallel running prior to the new or upgraded software being acceptable for use in the live environment.
ii. A parallel run phase should be incorporated in the User Acceptance Test Plan.
iii. In a scenario where two systems are running parallel, the maximum time for parallel running should not exceed six months.
iv. Where results differ between the old and new system, the old system should continue to be used until the new system is up and running, or otherwise agreed as acceptable.

5.5.5.6 Emergency Request Change

On occasion, changes of an "emergency" or critical nature may be required to quickly address production issues arising in case of emergency. Changes should be rectified urgently while still maintaining the proper levels of approval, logging, monitoring, communication and closure of all change related activities.

5.6 Prohibited Software

It is expressly forbidden to possess, distribute, reproduce or use computer programs for reasons such as scanning networks, intercepting information or password capture unless specific authority is obtained or held.

General Instruction for Software:

All Government executing agencies at a minimum shall be required to:

i. Use IT equipment and related products in line with the specifications laid down by the manufacturer;
ii. Procure/acquire IT hardware and software with proper and authentic certification;
iii. Keep record of all IT equipment supplied to facilitate future e-waste collection;
iv. For safe disposal of the IT products after their useful life and to separate e-waste generated by the products to facilitate collection, Handling and recycling;
v. Dispose e-waste generated by IT equipment after their useful life to the e-waste collection centers or designated area or place;
vi. Take back IT hardware equipment to the supplier or assembler, if they allow it after their useful life;
vii. Be responsible for following recommended disposal methods or procedures especially dates of expiry or end of usage period of the IT products (hardware & Software);
viii. In cases where the procuring executing agency has more than one location. The entity shall ensure that the IT Products (hardware & software) reach their pre-destined end user;
ix. A record of end users including the number of IT products procured within the entity should be kept and maintained.

General requirement for Software Procurement

The following guidelines shall be followed by the respective executing agencies:

- All software Procurement shall be done with consultation and coordination of the IT personnel's or experts within the respective executing agencies who shall be responsible for the preparation and issuance of all technical specifications for the software, as well as ensuring that the guidelines stipulated herein are adhered to;
- Executing agencies shall ensure that requests for procurement of software are validated by IT experts. Executing agencies shall also ensure that requirements are clearly defined and documented when procuring enterprise software. Where possible, executing agencies shall endeavour to use enterprise version of software;
- Executing agencies shall make sure that there is no already existing software application within Government that provides equivalent functions and that can be replicated in the organization before procuring any software to avoid duplication;
- All IT software procured or donated to executing agencies shall be received by the IT personnels who shall ensure proper custody and issuance. All donations shall be required to meet the minimum specifications. Further, all software and assets (new, transferred and/or written off) shall be recorded for audit and other managerial purposes;
- Executing agencies shall endeavour to procure and use the latest version of software. Where a previous version of software is to be used, executing agency's shall be required to give justifications;
- Technical evaluation shall be undertaken to ensure that the software is fit for the purpose it is being acquired for and that it meets the provided specifications. Upon delivery of the software, all inspection done so that they meet the laid down specifications. IT Personnel's shall ensure that technical evaluation and inspection reports are prepared respectively;
- IT Personnel's shall ensure that an agreement is in place to warrant software support and replacement when required, and that such agreements acquired are enforced.

CHAPTER SIX
Training

6.1 ICT Training

There should be provision of adequate training on ICT matters, as embedded in their working environment.

i. Modern facilities be built up to promote ICT education and computer-aided education.
ii. ICT training needs of government officials should be identified
iii. a customisable model should be created that adopts a holistic approach towards the effective ICT training of government officials (Customisable effective ICT training model);
iv. Raise awareness of effective ICT use among government officials that allow them to critically examine beliefs and develop powerful images of effective ICT use (Awareness of effective ICT use);
v. Design and implement curriculum for ICT training of government officials that is based on sound instructional design principles (ICT training curriculum design and implementation)
vi. Integrate ICT training curriculum in the training programme of government officials, i.e. ICT training is not a stand-alone, it should be integrated as part of the professional development of government officials (Integration of ICT training into overall professional development of government officials);
vii. Provide training for project management of ICT training projects;
viii. Proper / continued training will have to be given to all employees at different levels on regular basis.
ix. Qualified and skilled teachers/ speakers will be included in the training program(s) in order to train up employees up to the mark.
x. ICT personnel to be trained on the necessary steps to be taken in case of any exigency/ health security problem emerged in the ICT area.
xi. Support the building, networking and co-ordination of ICT training centres (ICT training centres);
xii. All the network users should be trained about its operating and security procedures.

6.1.1 Need Analysis

- Identify the gaps between actual and desired performances of government officials in the use of ICT.
- Identify the gaps between actual and desired state of professional development programme for ICT training of government officials.
- Acknowledge the language abilities and preferences of government officials, especially senior ones.
- Develop the concepts of ICT training for government officials.

6.1.2 Customizable Effective ICT training Model

- Provide a better linkage between professional development programme and the workplace.
- Create a balance between just-in-case training (basic repertoire of skills, attitude and knowledge) and just-in-time training.
- Complement formal training with informal/formal sharing sessions of best practices of ICT use.
- Provide opportunities for government officials to apply their newly acquired skills and knowledge in the workplace.

- Provide support and incentives for government officials to update and upgrade themselves as part of the lifelong learning process.
- Build a learning community within and across departments for effective ICT use among government officials.

6.1.3 Awareness of Effective ICT Use

- Create opportunities for government officials to examine critically their beliefs of ICT use in their workplace.
- Document and show best practices of ICT use in the workplace.
- Guide government officials to form visions of effective ICT use in their workplace.
- Highlight to the senior government officials their pivotal roles in effective ICT use and training.

6.1.4 ICT Training Curriculum Design and Implementation

- Design the curriculum for ICT training of government officials that is based on sound instructional design principles.
- Identify the opportunities and limitations of different medium of delivering training (e.g. online learning, CD-ROMs, textbooks, chats, discussion boards, face-to-face lectures and tutorials).
- Plan for and coordinate the outsourcing of training to private companies, higher education and vocational institutions, and overseas partners.
- Develop a database of training materials (online and offline, computer-based and non-computer-based), vendors, software, textbooks, services and opportunities available to government departments and officials.
- Allow for different learning paths for different officials with respect to a set of standards.

6.2 Training on information security

Adequate training of all personnel is critical to the effective implementation of information security. Security awareness and training activities should be ongoing to further demonstrate management's commitment to information security. The Management should be proactive in communicating its expectations and requirements to its personnel, as well as in prescribing disciplinary action for non-compliance. Users should be appropriately trained to perform their tasks prior to access to systems and information being granted. To give appropriate security training to executing agencies users, the users have been categorized into technical users, end-users and temporary employees/trainees.

a. Technical User

i. Technical users should be trained on security aspects for a new procured software and hardware.

ii. Regular training should be conducted to technical users; this includes systems analysts, designated system administrators and information security officers on the use of patches for existing software.

iii. Designated Information System Security officer should monitor and review the level of information security knowledge of technical and operation staff on regular basis. This can be achieved by introducing a bi-annual self-assessment form.

b. End User

i. End users should be trained on security aspects for a new procured software and hardware.

ii. End users should be given appropriate information security trainings on the latest security threats and information security techniques on regular basis.

c. Temporary Employees and Trainees

Temporary employees and trainees such as field students should adhere to the following requirements:

i. Attend induction training on security matters and sign non-disclosure agreement prior to accessing users.

ii. Attached to a selected location.

iii. Given limited access to the system.

CHAPTER SEVEN
Maintenance

7.1 Types of Maintenance

7.1.1 Maintenance

Regular IT maintenance keeps IT systems run smoothly. This section explores the regular IT tasks that should be implemented to maximise efficiency.

When we talk about maintenance, the aim is to:

- preserve IT systems in optimal condition
- fix problems that occur
- upgrade the existing systems to minimise future risks.

This will require maintenance of hardware, software and data.

7.1.2 Types of Maintenance

Maintenance falls into two broad categories:

- preventative (or routine maintenance)
- reactive (or non-routine)

Preventative Maintenance: We need to carry out preventative maintenance on a periodic basis to prevent problems occurring in the future. For example, periodically have we do car servicing, which involves changing the engine oil, air filter, spark plugs and so on. If we don’t do this, chances are at some later time car’s performance will suffer, and may even be stranded at a great inconvenience. This is preventative maintenance, and the situation is really quite similar with IT equipment.

Reactive maintenance: Reactive maintenance refers to actions taken to fix problems after they have occurred. To continue with the car example, when we get a flat tyre and have to replace it, this is a simple example of reactive maintenance. we can probably think of many IT examples. Replacing a broken cable is one. Apart from preventative and reactive maintenance, there is another type of maintenance that deals with upgrading the organisation’s infrastructure to minimise the level of risk to continuity.

7.2 Maintenance of Software

It’s not only the hardware in an organisation that needs to be maintained-software maintenance is also required. An organisation that has custom-built software needs programmers to maintain it. This will include:

- preventative maintenance to detect and correct code that may cause future errors (to validate input data)
- adaptive maintenance to adapt the software in line with changes to requirements (to make it run on an Intranet)
- perfective maintenance to simply improve the performance of the software
- reactive maintenance to fix software bugs.

But apart from custom-built software, organisations need to maintain other software. There may be patches, version updates, driver updates, etc to be installed. Upgrading packaged software across an organisation to standardise software versions is a good way of helping to reduce the level of support and maintenance required. Maintenance of a hard disk is really a form of software/ data maintenance. A variety of tools are available for 'cleaning up' a disk, removing unwanted programs and data, backing up data and so on. Protecting the system from viruses and malware is also part of this sort of maintenance.

7.3 Preventative Maintenance

Specific devices require different preventative maintenance procedures. However, there are a few broad areas that can be considered which require preventative maintenance practices. These include:

- Protection of equipment due to changes in electrical supply: Surges and 'brownouts' cause major damage to computer devices. Un-interruptible power supplies (UPS), power conditioners and surge protection devices are all valuable preventative maintenance tools for any computerised device.
- Protection from environmental conditions: Humidity, temperature variation and dust are major causes of computer device failures. Actions taken to limit these factors in the workplace are valuable preventative maintenance tasks.
- Protection of data using backups: It is vital that backups of both user data and system configurations are done regularly.
- Protection of data from threats: Data needs to be protected from viruses, malware, hackers and so on, through the use of both hardware and software security measures.
- Keeping software updated through service packs, patches and driver upgrades
- Checking integrity and performance by using diagnostic tools: Routine running of any in-built diagnostics and/or checking for display of maintenance messages generated by the device.

73.1 Protecting Critical Hardware (Facility Protection)

Strategies must be in place to protect IT equipment from water damage, fire, contamination, power failure and theft. Some of these strategies include:

- the implementation of early warning systems to detect water leaks, fire and air-borne contaminants
- devices to continue power supply should there be a power failure such as a UPS (uninterruptible power supply) as well as on-site power generation
- security access to computer facilities such as swipe cards or entry of a security number
- recording serial numbers, asset numbers, location and allocation details of workstations.

7.3.2 Redundancy

If part of a network is interrupted, critical processes need to be stored as soon as possible. One way of doing this is by implementing and maintaining full or partially redundant systems. This means having an identical hardware infrastructure that can be activated should the main hardware infrastructure fail. Redundant systems can range from the duplication of entire networks to the duplication of cabling runs. Where entire networks are duplicated, system backup facilities are not required. However, full network redundancy is extremely expensive and, as such, not a commonly used option.

- Partial redundancy is a common option for critical IT hardware.
- An organisation's disaster recovery plan will include such procedures for recovering network systems.

7.3.3 Protection from environmental conditions

a. **Temperature**

The tolerance of computer components for extremes in temperature is limited — subjecting them to temperatures outside this range is likely to reduce their life. The room environment as well as cooling and ventilation systems are, therefore, important in maintaining computer equipment in optimum operational condition.

b. **Humidity**

Computers are also sensitive to humidity and should be kept dry. Protective measures would include keeping them away from windows, and avoiding food and drinks spills. Ventilation systems also help prevent problems with humidity.

c. **Dirt and dust**

Computers should be kept in a clean environment. Dust build-up around fans and on electrical components becomes a problem because it tends to prevent heat dissipation, and interferes with the fan's cooling function. Regular cleaning is, therefore, important. If the equipment is kept in an industrial environment, additional measures must be put in place to protect it — use of air cleaners is one useful strategy.

d. **Cigarette smoke**

The particles from cigarette smoke have the same effect as dust — they build up on the surface of equipment, causing the same sorts of problems.

e. **Electromagnetic interference**

All electronic devices are capable of producing electromagnetic interference that can cause data to be lost, problems with picture quality on monitors, and other problems.

7.4 Protection of Data (backup)

All organisations need strategies in place to:

- backup critical data, and
- ensure that data backup is being undertaken according to organisational policies.

This will involve both server backup and workstation backup.

Server backup options

Backup option	**Benefits**	**Limitations**
Backup to tape using backup/restore software such as windows: the tape backups from the server can be sent to an off-site backup storage facility for restoration if backup files on-site are destroyed.	Simple; software readily available in Windows	Additional risks in transportation and storage; time to restore in the event of loss of data, ie time to data, can be too long and very costly
Backup server data to a remote tape unit via a WAN	Time to data much shorter; risks reduced due to less manual handling	Can be expensive
Backup data to a remote mirrored disk via a WAN	Time to data instantaneous; risks lowered further	Costs are high

7.4.1 Workstation Backup

Workstations in an organisation are often standardised with respect to operating system and common applications. An ‘image’ or ‘build’ is created, making it much easier to restore the workstation to a re-usable state. There is usually an IT policy that specifies a ‘Standard Operating Environment’ for workplace PCs. Uncommon, or specific, applications are usually installed separately after the standard image is loaded. However, users tend to customise their PCs with shortcuts, background images and screensavers, taskbar options, mouse speed and a variety of other options. Also, though it may be against company policy, there may be company data lurking on a user’s PC. Therefore, before any changes are made to a workstation PC, the hard disk should be backed up. As mentioned, staff in a client/server organisation are generally encouraged not to store data on their own hard drives. However, where an agency’s data is stored on a workstation hard drive, there must be some procedure in place for regularly backing it up.

Types of backup

An agency will have policies that relate to:

- the frequency of backups (daily, weekly, monthly)
- the time of day backups are done
- how long backups are kept
- where backups should be stored.

Also, there are different types of backup. Different options include:

- backup of selected directories
- incremental backup – backup of only files that have been created or changed since the last full or incremental backup
- differential backup – backup of files that have been created or changed since the last full backup.

a. Backup scheduling

Backup scheduling is an important part of any preventative maintenance plan. Windows provides a backup and restore tool, and this type of software is also provided by third parties.

b. Protection of data from threats

Because of the widespread interconnectivity of computers today, and the potential for intrusion, theft, damage, and so on, organisations need to have clear policies and procedures to be followed to minimise these threats.

c. Service packs, patches and operating system updates

It has become obvious in recent years that when operating systems are released, they are not finished products. Because they are so complex, even after a period of rigorous testing, security flaws are often discovered after distribution. Anti-virus and other security tools cannot protect the system from operating system holes. For critical security holes, as soon as the flaw is discovered, the software manufacturer quickly develops and releases a patch, which is a small software update to eliminate the hole. A group of patches is sometimes released as a major update, or service pack.

d. Anti-malware software

Malware has increased in significance over recent years. Included in this category are:

- Trojans, which appear to be harmless programs, are actually designed to either do damage or carry out a range of malicious activities

- Worms, generally spread as email attachments
- Spyware, adware and browser hijackers collect information from computer or change the Internet options in the browser.

Anti-malware software helps to prevent a computer from these attacks. However, installing it and forgetting about it provides insufficient protection. Regular updates need to be carried out.

e. Antivirus software

Viruses have been around for a long while, and have been overtaken somewhat by other types of threat. However, using antivirus software which is regularly updated is still an important preventative maintenance measure for computer systems.

f. Firewalls

There are two types of firewalls — hardware and software firewalls. **Hardware firewalls** offer the best protection against intrusion, but they are expensive for small companies. Desktop or a **software firewall** is useful, but malicious software may find ways to bypass it.

7.4.2 Keeping software updated

Often a device is purchased with a projected life of several years, but in the mean time, other equipment and operating systems that it is used with are updated. Sometimes this means that a perfectly good piece of equipment no longer works, or works unsatisfactorily. So new software for these devices (drivers) is developed and released. Keeping abreast of these various driver updates is also important in preventing problems before they arise.

7.4.3 Checking integrity and performance

Computer operating systems are generally provided with an array of diagnostic tools that can be used to check whether there are either hardware or software problems with the machine, or whether steps can be taken to improve its performance. For example, Disk Defragmenter and Disk Cleanup are tools available in Windows operating systems. A whole range of other utilities is also available from other software manufacturers.

7.4.4 Determining organisation's maintenance requirements

To start with, organisation will have specific procedures that deal with maintenance and how it is scheduled. These procedures will be either as a result of, or in conjunction, with the following:

- Organisational policies, for example, a particular procedure may be in place because of organisation's policy on the management of risk.
- Equipment, in particular specialised equipment, is covered by warranties and maintenance contracts. These will often involve an agreed level of support for the equipment, also called a service level agreement (SLA).
- Both equipment and software are provided with documentation regarding their handling and maintenance requirements.
- Support is also often provided by phone or website, and may even involve the provision of training.
- There is a service level agreement.

7.5 External Service Level Agreements

Maintenance agreements are a way of ensuring support to an agreed level at a known cost. All critical hardware components and software should be covered by either a warranty or maintenance agreement. There are a number of things to consider:

1 New purchases: A warranty agreement comes automatically with the purchase of hardware components and software.
2 Extension of warranty: One can enter into a maintenance agreement when the initial warranty expires rather than extending the warranty.
3 Type of cover: A maintenance agreement is an agreement negotiated between the organisation and the supplier to maintain the hardware or software. Maintenance agreements can be on a fixed service basis, eg 24 hours a day, 7 days per week (24/7); 8 hours a day, 5 days a week (8/5); 12 hours a day, 5 days a week (12/5) or on a per-call basis.

7.5.1 Software warranties and maintenance agreements

Software should also be covered by a warranty or maintenance agreement. Software warranty only lasts for a short period of time, so a maintenance agreement for critical software should be in place. If customised software has been developed in-house, a maintenance agreement will not be necessary because it will be maintained internally. A software maintenance agreement may include, for example, a free or discounted upgrade of packaged software.

7.5.2 Common hardware maintenance tasks

While it is beyond this topic to identify all types of maintenance across the range of devices available in the IT workplace, the following devices and preventative maintenance tasks are included here as common tasks.

Cleaning

The following table gives suggestions for cleaning the parts of a computer.

Device	**Type of maintenance**	**Resources**
Keyboard	Keyboard covers; regular 'dusting' with compressed air	Original system documentation will recommend cleaning material instructions
Mouse	Cleaning mouse ball and rollers; replacing ball mice with optical mice will solve most problems	Original system documentation will recommend cleaning materials
Monitor	Wiping of screen — be careful of the cleaning products used as some may damage the screen. Consult the manufacturer's instructions for the monitor.	Original documentation will recommend cleaning materials
CD/DVD drives	Cleaning drives with CD/DVD cleaning kit	CD/DVD cleaning kit documentation
Floppy disk drives	Cleaning drives with FDD cleaning kit	FDD cleaning kit documentation

7.5.3 Whole system maintenance

Maintenance of a computer system will also involve:

- checking system event logs regularly

- viewing POST results
- routine checking using system monitoring utilities that track system temperatures, voltages and fan speeds
- checking for dust accumulation, particularly around fans and vents
- updating drivers for printers, modems, soundcards, video cards and so on, as needed
- updating operating system and application software with the latest service packs; eg later versions of Windows allow updates to be automatically downloaded and installed, but this can be disabled
- updating anti-virus software and virus definitions.

7.5.4 Hard disk maintenance

Software for carrying out hard disk maintenance is provided by the operating system utilities, as well as by third party software. Typical maintenance will include:

- removal of unwanted files — this can include old files, temporary files, downloaded files, corrupt files, Internet cookies, and browser history
- removal (uninstalling) of unwanted software
- backup — this may be by means of standard backup/restore software, or through imaging software such as Norton Ghost
- cleaning up the registry
- defragmenting files
- creating system restore/boot disks
- scanning for viruses, spyware, adware, malware, and so on
- disk checking using standard diagnostic tests.

Many of these activities can be scheduled to occur automatically. We'll discuss scheduling in the next section.

7.5.5 Printers

Most maintenance on printers relates to **print quality** and **paper handling**. Maintenance on printers may include the following.

Component	**Type of maintenance**	**Resources**
Laser printer drum	Cleaning/replacement. Some printer replacement cartridges include the drum, requiring less maintenance. Others may require a separate maintenance procedure for the drum. Consult the manufacturer's instructions.	Printer documentation
Ink print heads	Cleaning/replacement. Some printer replacement cartridges include the ink print heads, requiring less maintenance. Others may require a separate maintenance procedure. Some print heads also require alignment. Consult the manufacturer's instructions.	Printer documentation, in-built printer cleaning utilities
Paper rollers and feed path	Purchasing quality paper, ensuring a dust free environment and regular cleaning. Consult the manufacturer's instructions.	Printer documentation

7.5.6 Tape backup systems

Tape backup systems are listed as a separate item here due to their importance in the IT workplace.

Device	**Type of maintenance**	**Resources**

Tape drive	Cleaning drive heads. This should be done regularly. Consult the manufacturer's instructions.	Head cleaning kit and original tape drive documentation
Backup software	Regular viewing of backup logs for errors	Backup software documentation
Tape media	Checking media for errors and tape age against the recommended tape life. Perform test restores to confirm reliability of media and backup process.	Backup software documentation and media specifications

7.5.7 Low maintenance devices

Many devices such as hubs/switches, scanners and USB devices are normally considered 'maintenance free'. However, these units may benefit from the following types of maintenance.

Device	Type of maintenance	Resources
Hub/switch	Checking systems log and port statistics for large error counts	Original manufacturer's documentation
Scanner	Glass cleaning with recommended products; ensuring a dust free environment	Viewing POST diagnostics test results
Other devices	Viewing POST diagnostics test results; running regular tasks to ensure the device is functional	Viewing POST diagnostics test results

7.6 Maintenance Scheduling

Many organisations with a preventative maintenance program will have maintenance tasks organised on a schedule. The goal of a schedule is to ensure that regular maintenance occurs. Given the time pressures of working as an IT Support person, a schedule will assist in organising workload to ensure that the best possible service is provided to the client. If a maintenance schedule does not exist, consider designing one. A schedule should simply include:

1 each preventative maintenance task that should be completed
2 how often the task should be repeated
3 an estimate of the time required to complete the task.

These tasks can then be allocated time in schedule at the required intervals.

7.6.1 Developing a preventative maintenance schedule

In developing a preventative maintenance schedule, it is important that as an IT Support person are aware of the main aims of preventative maintenance. They are:

- to meet the needs
- to extend the working life of equipment
- to reduce the amount of emergency downtime caused by faults that can be prevented
- to be practical
- to make the IT system more cost effective.

7.6.2 Cost effectiveness

It is important that any preventative maintenance be cost effective. It is possible to spend significant amounts of time cleaning and testing devices such as keyboards and mice to extend their life. However, the replacement cost of those devices, including the cost of having an inventory of such items on hand, may mean that it is cheaper to purchase new devices rather than extend the life of the existing devices. Every maintenance issue must be examined from a cost point of view.

7.6.3 Minimise downtime

It is important that preventative maintenance focuses on items that may cause significant downtime and cost to the work if they were to fail. Such items may include hard disk drives (HDD) of servers. Should they fail, emergency downtime may occur at a significant cost to the work. As a result, such devices should be considered high priority in a maintenance schedule.

7.6.4 Practicality

Preventative maintenance must be practical within the work. If the process of preventative maintenance causes a major interruption to the daily work, the maintenance program will fail. Always try to consider the impact on the users of the computers when considering a preventative maintenance program.

7.6.5 Timing for tasks be scheduled

Scheduled maintenance should obviously impact as little as possible on normal operations, and should therefore be carried out at periods of low activity, such as during the night, at weekends or holiday periods. It is possible to carry out many tasks with very little client awareness or involvement. If client involvement is required, they should be informed in advance of when they will be affected, for how long, and how it will impact them. One may need to give them instructions, such as logging out of their PC, leaving it on, rebooting, and so on. There are some useful operating system or third-party tools which allow maintenance tasks to be automatically scheduled. This is the case with later versions of Windows.

7.6.6 Frequency of tasks be scheduled

To determine how frequently maintenance tasks should be done, should first refer to the types of documentation mentioned earlier in this topic. The preventative maintenance strategies in place would also help determine the frequency of tasks. One should also bear in mind the principles listed above.

.

Scheduling can be a formal process, where preventative maintenance is carefully scheduled for various units within the organisation and formally documented and signed off. It can also be an informal process.

The following should be documented in a preventative maintenance schedule:

1 dates for maintenance to occur
2 unit/floor/building/computer facilities where the maintenance will occur
3 the IT staff member responsible for completing the maintenance
4 dates for completion
5 notification that maintenance has been completed
6 comments or notes where problems are detected.

Preventative maintenance schedule will occasionally alert to potential problems. When this happens, One should be aware of the appropriate person to inform.

CHAPTER EIGHT
Recommendation

IMED officials may use the Guideline to get accustomed with suggested specifications for Hardware, Cloud Computing, Website and Data Center.

IMED officials may use the checklists of the Guideline for Web Applications, Information Security Documentation, Incident Response Plans, Vulnerability Analysis, System Continuity and Disaster Recovery; Servers and Network Devices; Software Application Development and Access Control.

IMED officials may use the Guideline to ensure that executing agencies are complying with the minimum requirements while acquiring different software such as Total Lifecycle Cost, Maintainability, Interoperability, Portability, Scalability, Availability, Accessibility, Reusability, Functionality, Performance and Security.

Where IT equipment or products exhibit characteristics, it shall be considered non- compliant: the product is not complete and some essential parts are missing; functionality or safety is impaired; the appearance is generally worn or damaged; it is destined for disposal or recycling instead of use; and it is old or outdated destined to be cannibalized to gain spare parts.

IMED officials need to follow the steps for handling procurement of ICT Services with a view to monitor and evaluate implementation of ICT components.

Procuring agency officials need to procure ICT goods and services responsibility in accordance with the Government's Procurement Rules and Acts.

Physical and Environmental security should aim at protecting executing agencies ICT facilities like hardware, software, data and communication infrastructure from unauthorized access, hazards, intentional or unintentional damage, as well as theft.

Breach of physical and environmental security may lead to loss of confidentiality, integrity, and availability of information systems assets. To prevent such loss, measures such as adequate air conditioning, fire detection and suppression systems, reliable power supplies, controlling physical access and suitable emergency preparedness should be in place.

Technical evaluation should be undertaken to ensure that the ICT services are fit for the purpose it is being acquired for and that it meets the provided specifications.

Upon delivery of the ICT goods and services, all inspection should be done by procuring agencies so that they meet the laid down specifications and appropriate training are being provided.

IMED officials may use the Guideline to ensure that technical evaluation and inspection reports are prepared respectively.

IMED officials may use the Guideline to ensure that an agreement is in place to warrant ICT support and replacement when required, and that such agreements acquired are enforced.

ANNEXURE – 1

Checklist for DPP

1. Project Title:
2. Objectives of the project:
3. Estimated cost of the project total GoB and PA (RPA):
4. Mode of financing:
5. Components of the project:

Sl.	Aspects to be answered/covered	Yes/No	Remarks
6.	Whether log frame in the DPP is correctly drawn to achieve the objective of the project?		
7a.	Whether required manpower as mentioned in the DPP has been deputed from existing setup, recruited directly or recruited by outsourcing?		
7b.	Whether recruitment of personnel has been made following government recruitment rules and regulations?		
7c.	Whether recruited/deputed personnel have requisite qualification and experience as mentioned in the DPP?		
8.	Whether there is a steering committee and PIC for reviewing the progress of project (monthly/quarterly/half yearly)?		
9.	Whether procurement plan of goods, works and services as mentioned in the Annex III (a), III (b) and III(c) are being executed following the PPA-2006 and PPR-2008.		
10a.	Whether item wise physical components as approved in the project document, differ from those being executed in the field.		
10b.	Whether physical components targets and progress as reported in the 02, 03 IMED formats are consistent with the field up to last quarter.		
10c.	Whether year wise financial phasing as approved in the DPP matches with the yearly ADP allocation.		
10d.	Whether year wise fund release and expenditure are consistent with the reported figures in the IMED formats.		
11a.	Whether project authority has clearly identified the RPA expenditure items of the project.		
11b.	Whether claims of RPA expenditures are being submitted quickly for reimbursement.		
12.	Whether benefit-cost ratio (BCR), net present value (NPV) and internal rate of return (IRR) figures provided in the approved project document are inconsistent with the present figures (for completed profit earning industries).		

Sl.	Aspects to be answered/covered	Yes/No	Remarks
13a.	Whether mitigation programs for environmental impact has been taken care of by the project authority as mentioned in the DPP.		
13b.	Whether the project in anyway is contributing to the poverty alleviation, empowerment of women and regional disparity as mentioned in the DPP.		
14.	Whether the project is contributing to the SDGs as mentioned in the DPP.		
15.	Whether any project aid conditionality mentioned in the DPP is affecting implementation of the project.		
16a.	Whether rehabilitation/resettlement of affected persons/families program is taken up by the project authority.		
16b.	Whether the cost involvement as mentioned in the DPP for rehabilitation/resettlement will remain within the approved estimate.		
17.	Whether project implementation period is likely to be extended		
18.	Whether there is a possibility of time over run and cost over run		
19.	Whether internal and external audits are being carried out. When last internal and external audit was done.		
20.	Whether site register/book is being maintained at project site and visiting supervisory officials are recording their observations on progress and quality of work etc.		
21.	Whether Annual Work Plan has been prepared by the project authority/PD.		
22.	Whether CPM/ Bar Chart, for smooth execution of the project, has been prepared and being followed.		

ANNEXURE - 2
Checklist for TPP

1. Project Title:
2. Objectives of the project:
3. Estimated cost of the project total GoB PA (RPA):
4. Mode of financing:
5. Components of the project:

Sl.	Aspects to be answered/covered	Yes/No	Remarks
6.	Whether there is a possibility for cost and time overrun.		
7.	Whether PD/NPD is a full time or a part time appointee.		
8.	Whether financing arrangement has been finalized.		
9.	Whether loan/credit/grant and other amounts as approved in the TPP is the same		
10.	Whether TOR of the consultants adequately covers the areas related to the objective of the TPP		
11.	Whether PPR 2008/ applicable procurement guideline in the TPP has been followed in selecting consultants		
12.	Whether adequate step have been taken by the project authority to ensure transfer of technology.		
13.	Whether consultant's performance is being monitored regularly		
14.	Whether educational qualifications and experience of the consultants are relevant to the assignments they have been engaged.		
15.	Whether the counter-part personnel attached to the consultants have required educational qualifications and experience as mentioned in the approved TPP.		
16.	Whether educational qualification and experience of the support staff matches with information provided in the approved TPP.		

Sl.	Aspects to be answered/covered	Yes/No	Remarks
17.	Whether letter of agreement with implementing agency and the development partner has been signed.		
18.	Whether project steering committee has been formed to review the progress of work.		
19.	Whether auditing of the project is being carried out. When the last audit was done?		
20.	Whether project work is progressing as per approved implementation works schedule provided in the TPP.		
21.	Whether total procurement plan as envisaged in the approved TPP is being implemented in the light of PPR 2008.		
22.	Whether approving authority is exercising financial authority as per Delegation of Financial Power published by ministry of finance.		
23.	Whether CPM/ Bar Chart, for smooth execution of the project, has been prepared and being followed.		

ANNEXURE - 3
Checklist for Procurement of ICT

Part-I: General

Ministry/Division	
Agency	
Procuring Entity	
Description of Procurement	
Estimated cost of the procurement/Official cost estimate	
Procurement Type	NCT/ ICT
Category of Procurement	Goods/ Works/ Services/ PSN
Method of Procurement	OTM/ LTM/ OSTETM/ TSTM/ RFQM/ DPM
	QCBS/ FBS/ LCS/ SSS/ ICS/ CQBS/ CSOS/ DCS/ QBS etc.
Object of Procurement	
Financing Arrangement of the Procurement	Revenue/Development

Part-2: Schedule of activities

Date of approval of Annual Procurement Plan (APP) :

	Aspects		Planned date (as per Annual procurement Plan	Actual
1.0	**Procurement Opportunities**			
1.1	Date of advertisement of IFT/EOI in newspaper (NCT/ICT)	:		
1.2	Date of advertised in CPTUs website/ dg Market	:		
1.3	Tenders/Proposals followed PPR, 2008 or e-GP guideline	:		
1.4	Tenders/Proposals followed DP's Guidelines	:		
2.0	**Tenders/Proposals Submission**			
2.1	No of Sale/Issuance of Tender/Proposal Documents	:		
2.2	No of Tenderer/Consultant participated (Submission)	:		
2.3	Days allowed per Rule for Preparation and Submission	:		
3.0	**Formation of TOC/POC and TEC/PEC**			
3.1	No of members in TOC/POC	:		
3.2	No of member in TOC/POC from TEC/PEC	:		
3.3	Approval date of TOC/POC	:		
3.4	No of members in TEC/PEC	:		
3.5	No of external members in TEC/PEC	:		
3.5	Authority approved TEC/PEC with date	:		
4.0	**Tenders/Proposals Evaluation**			
4.1	Days allowed in tender/proposal documents for preparation, submission and opening	:		
4.2	Actual days between opening and completion/submission of evaluation	:		

	Aspects		Planned date (as per Annual procurement Plan	Actual
4.3	No of responsive tenders/proposals	:		
4.4	No of non-responsive tenders/proposals with reasons	:		
4.5	Re-invitation of tenders/proposals recommended by TEC/PEC	:		
4.6	Procurement proceedings annulled/cancelled	:		
5.0	**Approval of Tenders/Proposals**			
5.1	Days actual between submission of evaluation and approval	:		
5.2	Approving Authority(AA) as per DoFP	:		
5.3	Authority approved	:		
5.4	Evaluation report was sent as per PPR to the AA	:		
5.5	Date of approval decision received by PE	:		
5.6	Date of issuance of NOA/PO/LOI	:		
5.7	Authority other than AA, if any, made additional review of the evaluation report	:		
5.8	Authority higher or lower than AA, if any, approved the Tenders/Proposals	:		
6.0	**Contract Award**			
6.1	Procurement processing lag/lead-time (i.e. Days actual between opening and issuance of NOA/PO/LOI)	:		
6.2	Days actual between IFT/RFP and issuance of NOA/PO/ LOI contract signing	:		
6.3	Contract award made within the initial tender/proposal validity period	:		
6.4	Publication of award in CPTUs website/PE's website/others	:		

Part-C: Individual Contract Review

Contract Name, Number and Date	
Contract Signing Date	
Contract Amount	

1.0	**Completion of Contract**		
1.1	Days per original contract time specified for Supply/Execution/Perform	:	
1.2	Days actual for Supply/Execution/Perform	:	
1.3	Amount of LD imposed (if any)	:	
2.0	**Complaints and Appeal**		
2.1	Complaint, if any, lodged and reasons thereof	:	
2.2	Resolution of complaints per Rules	:	
2.3	Modifications resulting from resolution of complaints	:	
2.4	Appeal to Independent Review Panel	:	
2.5	Review Panel's decision and follow-on	:	
3.0	**Contract Amendment**		
3.1	No of times contract completion period extended and with no of days	:	
3.2	Variation/Extra Work/Repeat/Additional Delivery Orders/ replacement of Key Personals etc. made	:	
3.3	No and amount of such orders	:	
4.0	**Contract Disputes unresolved**	:	
5.0	**Fraudulence and Corruption**	:	
6.0	**Procurement Management Capacity**	:	
6.1	HRD facilities	:	
6.2	No of Staff trained in procurement	:	

ANNEXURE - 4

Checklist for Requirement Analysis

No	Section	Activities
1	Background	Information about the general factors that affect the products and their requirements • Function and purpose • Environmental considerations • physical, hardware, operating environments • Specify where system is to be used and by whom; networks and platforms involved; operation in different member states etc. • Relation to other systems - state whether the system is independent, subsystem of a larger one or a replacement • Model • logical model at all levels, explained top-down • describe functionality at all levels • provide means to 'walk through' model level-by-level, function-by-function and flow-by-flow • Relationship to other projects • put project in context of others past, present or future • identify 'parent' projects or project(s) being replaced • identify applications, tools and techniques • General constraints • identify limitations on options for building software • provide background information to justify constraints • consider applications, tools and techniques from other projects especially horizontal actions and measures
2	Specific requirements	Information about project requirements: • Overview • provide complete top-level statement of products and services to be delivered • include pre-development services (eg requirements analysis), hardware, software, documentation, training, warranty etc • provide overview of specific requirements pertaining to these deliverables • Detailed requirements structured top-down • consider using requirements specification language • only one requirement in each statement • requirements must be verifiable • some requirements may have to be provisional • requirements to be marked essential or non-essential • prioritize requirements • Pre-development services

		• describe services to be procured at the same time as main system development • examples are: Feasibility study, Benchmarking study, Requirements Analysis, Project Planning, Evaluation of available products, Technological trials, Development of demonstrator (system mock-up)
3	Hardware requirements	If the contract delivers hardware, specify requirements for each item of equipment; specify: type, number, functionality, standards, interfaces, performance, capacity, expansibility, reliability, availability, durability, maintainability, running cost limitations, operational requirements etc
5	System capability	Sets of requirements to be described • Functional – purpose of system Interfaces • Software: e.g., operating systems, software environments, file formats, database management systems and other software applications • Hardware: hardware configurations • Communications: for example, use of a particular network protocol • External interface requirements should be described or referenced in Interface documents. User interface requirements should be specified under 'Operational requirements'. Interface requirements can be illustrated with system block diagrams Operational • running of system and its communication with users • include all user interface and interactions • include also logistical and organizational requirements (examples screen layouts, error message contents etc) Security • protect against threats to confidentiality, integrity and availability • take account of physical and electronic protective measure • particular attention to telecommunication related security requirements, e.g. encryption, authentication, virus attack Safety – managing damage from system failure Quality – ensuring system is fit for purpose
6	Operational characteristics	Requirements about system performance: • Capacity: physical resources required eg processing power, memory, disc space etc; include expansibility • Performance: must be quantitative, not qualitative, statements; possibly include worst/best cases and nominal value to be used for planning • Availability: details of days/times, tolerable breaks, system failure notification, usage during failure and availability monitoring

		• Reliability: acceptable mean time between failure (MTBF), minimum acceptable MTBF; reliability verification
7	System architecture	Requirements specifically affecting the system architecture itself: • Maintainability – fault repair and adaptability in quantitative terms; influence of user availability/adaptability • Portability – software ability to work on other (named) systems • Prescribed components– applications, tools and techniques available from other projects and OSNs; consider Horizontal Actions and Measures • Software constitution and structure– name actual products
8	Documentation	Requirements for project-specific documentation, including number of copies and medium of documentation. • Documents may include user training, user reference, system management, operational support, release notes, configuration control files, system maintenance, supplier reference, warranties
9	Other services	Requirements for services commissioned for provision during or after development. Need to specify for each: when detailed specification will be produced; procedure for approving these specifications; responsiveness and level of service to be provided by contractor; complaints and disputes procedure. Examples (not exhaustive) are: • Training – specific courses, training material for users, support staff, system operators, maintainers and trainers • Installation processes – supply and delivery methods • Parallel running – developer involvement, if any • Operational support – developer provision, if any • Warranty – validity criteria for, and procedure to invoke, warranty; levels of service for corrections and warranty for corrections • Maintenance– developer's obligations outside warranty including procedures for upgrades and system changes
10	Developmental requirements	Requirements relating to the conduct of the contract: • Roles and responsibilities – details of team's structure and roles to include points of contact, people with decision authority and quality control mechanisms • Phases– timing details for product delivery • Verification– details of constraints on how system will be verified, e.g. testing location, performers and timings; dispute resolution; validation of system against user needs
11	Requirements traceability matrix	Tabular information summarizing how each requirement from User Requirement has been met in System Requirement document

ANNEXURE - 5
Checklist for In-depth Monitoring of ICT Projects

1	Ministry/ Division	
2	Implementing Agency	
3	Project Name and ID	
4	Expected Project Completion Date as per DPP/TPP	
5	Date of Commencement	
6	Expected Date of Completion	
7	Expected Expenditure	
8	Development Partner Name (if any)	
9	Brief Description of Project Components	
10	Major ICT Components	
11	Procurement Method Used	
12	Date of NOA Issued	
13	Date of Contract Signing	
14	Number of time extension (if any)	
15	Total Physical Progress	
16	Total Financial Progress	
17	Cost Overrun (if any)	
18	Stage of Project Work	• Less than 1 year • 1 to 2 year • More than 2 year

ICT Infrastructure Development

	CPM of the project available?	**Remarks**
	Gantt Chart of the project activities are available at field?	
	Are funds being released on time?	
	How many times Project Director has been changed?	
	Is land requisition been completed within specified timeline?	
	Availability of Approved Drawing	
	Are the roles of the building and its various rooms adequately defined?	
	Construction started as per approved drawing?	

	If not Available, reasons for unavailability.	
	Infrastructures development (focusing on ICT usage)	
	Have plans been prepared focusing on different ICT rooms that will be built through the project?	
	Total number, type, size and other construction-related technical requirements such as raised floors, etc.?	
	Do ceiling constructions have sufficient strength to support ceiling-mounted equipment (ICT rooms and stages)?	
	Electrical power requirements (normal power supply, stand-by power supply, uninterruptible power supply, redundancy)?	
	Cooling and ventilation requirements (redundancy) for controlling temperature?	
	Fire detection and extinguishing requirements?	
	Security requirements (access control, camera surveillance, etc.)?	
	Lighting requirements, etc.as per need?	
	What are the protective measures taken to secure equipment?	
	Deployment of Manpower	
	Manpower of contractor as per contract.	
	Manpower of consultant as per contract (if any).	
	Mobilization of construction material at site	
	The quality of construction material used for infrastructure development (test reports/ evidence) approved by authority.	
	Foundation work designs been provided on time?	
	Is Foundation work progressing as per contract agreement?	
	Is Foundation work progressing as per process flow diagram?	
	Is the quality work/ sustainability ensured?	
	Number of foundation completed as per schedule.	
	Progress of work	
	Construction work progressing as per work schedule prepared.	
	Monthly/ quarterly/ yearly work progress for construction work.	
	Record Keeping	
	Maintaining site work register book/ document and checked by authorized supervisor officer.	
	Maintaining and recorded manufactures manual.	
	Maintaining all test reports and records including material tests and collected	

	sample reports.	
	Deviations	
	Financial Progress is consistence with the physical progress in the field.	
	Any major deviation in the scope of project.	
	Any major deviation of the contract agreement.	
	Any major deviation of approved DPP.	

IT Furniture Procurement Monitoring		**Review Outcome**		
		Yes	**No**	**Remarks**
1	Does the procurement process follow PPR 2008?			
2	Are furniture's procured are compatible of range of users and ICT equipment's?			
3	How do you define the quality of furniture? (Excellent, Good, Poor)			
4	Is the product delivered in estimated time?			
5	Who is the responsible person to accept the furniture delivery?			
6	Is the furniture delivered according to specification?			
7	How faulty furniture is replaced?			

ICT Project Background Analysis	**Review Outcome**		
(Information about the general factors that affect the IT products and their requirements)	**Yes**	**No**	**Remarks**
Has the feasibility study been done? (specifying the target group, functionality)			
Is Feasibility study, Benchmarking study, Requirements Analysis, Project Planning, Evaluation of available products, Technological trials done?			
Does the IT component fulfil the objectives of the project?			
Is the ICT component is compatible with latest technology?			
Is Hardware requirement prepared by an ICT personnel?			

ICT Project Background Analysis (Information about the general factors that affect the IT products and their requirements)	Review Outcome		
	Yes	No	Remarks
Specify where system is to be used and by whom.			
User Group and total user number of IT component identified?			
Identify relation to other systems - state whether the system is independent, subsystem of a larger one or a replacement.			
Identify functionality of the system at all levels.			
Identify relationship to other projects (put project in context of others past, present or future).			
Identify limitations of IT component of the project			
Provide background information to justify constraints			
Justify the sustainability of the project in regard of software and hardware and the need of stakeholders			
Identify the product lifecycle associated with user need			
Estimated time for delivery of product			
Is function and purpose of the system defined?			
Is the human resource identified to run the IT component?			
Are user documentation and training requirements addressed?			
Is risk identification and risk management done?			
Is Cost analysis of IT components done?			
Is strategic plan for implementation done?			
Is the total number of system user identified?			
Is approximate life span of the system identified?			
Is system requirement is identified with justification?			
Is there any technological barriers identified?			
Are all significant consumers of scarce resources (memory, network bandwidth, processor capacity, etc.) identified, and is their anticipated resource consumption specified?			
Applicable timing, resource usage (e.g., CPU, memory, bandwidth), and associated system load requirements are			

ICT Project Background Analysis **(Information about the general factors that affect the IT products and their requirements)**	**Review Outcome**		
	Yes	**No**	**Remarks**
identified.			
Have all dependencies on other systems been identified? (Applications or application interfaces, databases, communications subsystems, networking, etc.)			
If the contract delivers hardware, specify requirements for each item of equipment; (specify: type, number, functionality, standards, interfaces, performance, capacity, expansibility, reliability, availability, durability, maintainability, running cost limitations, operational requirements etc.)			
Specify networks and platforms involved.			
Have all dependencies on other systems been identified? (Applications or application interfaces, databases, communications subsystems, networking, etc.).			
Has Software Requirement Specification done along with User Requirements analysis, Technical requirements, design description and format of Forms and GUI screen prints?			
Is there any default pay back if any vendor unable to deliver the product in estimated time?			
All functional capabilities are documented.			
All adaptation requirements identified (e.g., geographic parameters, platform variations are identified).			
Applicable safety requirements are identified.			
Applicable security requirements are identified.			
Applicable acceptance criteria (e.g., test, inspection, demonstration) are identified.			
Specify all modules and functions of IT component			
Are all diagrams provided before ICT components implementation?			
Is the project in compliance with IT Infrastructure Standards?			
Is the project in compliance with National Enterprise Architecture?			
Is all module completed as per diagram?			
How Support and maintenance support and maintenance of the			

ICT Project Background Analysis **(Information about the general factors that affect the IT products and their requirements)**	**Review Outcome**		
	Yes	**No**	**Remarks**
system will be done?			
What constrains are faced during implementation and steps taken to solve the constrains			

Software Monitoring	**Review Outcome**		
	Yes	**No**	**Remarks**
Is requirement analysis done before software development?			
What the kind of applications, tools and techniques to be used for software development? (as pricing of software vary with tools used)			
The kind of software procured			
Is all step are followed as per documentation/ software design?			
Is all modules are developed as per contract?			
Is software development is doing progress as per gannt chart?			
What is current percentage of development regards to total software?			
What is the financial progress of the software development component			
Is there any constrain faced during software development phase? How is it addressed?			
Is software administrative power/ user is handed over to implementing agency? (if required)			
Is source code and all design documentation is hand over to the authority after the software developed?			
Have all quality attributes (characteristics) been properly specified (i.e. efficiency, flexibility, interoperability, maintainability, portability, reusability, usability, availability)?			
Has full life cycle support been addressed, including maintenance?			
Is there any pay backs if software development company could not complete the software development in stipulated time?			
Is the software performing fully as estimated capacity as per requirement analysis in time of software delivery?			

How Software maintenance support is ensured?			
Reuse of existing software is fully described.			
Is all software design documents and user documents are hand over to the implementing agency?			

Hardware Monitoring	**Review Outcome**		
	Yes	**No**	**Remarks**
Is the ICT component is compatible with latest technology?			
Hardware requirement was prepared by an ICT personnel?			
Is any technical person revived the procured hardware?			
Is the specifications are matched with the specifications written in tender?			
What is the total life span of the major procured hardware?			
Is hardware procurement is in progress as per gannt chart?			
What is current percentage of development regards to total software procurement?			
What is the financial progress of the software procurement component?			
Is there any constrain faced regarding hardware procurement?			
How maintenance and support ensured?			
Is support and maintenance book maintained?			

Technical Assistance/ Consultant Recruitment Monitoring	**Review Outcome**		
	Yes	**No**	**Remarks**
Is any need assessment done to find to relevancy of Technical Assistance/ Consultant Recruitment for specified component of the project?			
Is the qualification of the Technical Assistance/ Consultant specified in TOR comply with need assessment?			
Is the recruitment done as per schedule of CPM?			
Is specific deliverables identified for consultant?			
Is consultant closely monitor the system development, progress according to schedule and performance?			
Do consultant prepare monthly, quarterly and yearly report for specified system?			

Security Measures Monitoring	**Review Outcome**		
	Yes	**No**	**Remarks**
Is Physical and Environmental Security measures taken (against fire, water, temperature)?			
Is uninterrupted power supply is ensured?			
Is access control measure is taken (for both physical and logical access control)?			
Is administrative power of a system given to authorized person of implementing agency?			

Is data or information security ensured at highest level?			
Is measures taken to protect the system against cyber-attack/ malicious viruses?			
How system surveillance is ensured (by alarm, sms, email etc.)?			

Maintenance Measures Monitoring	**Review Outcome**		
	Yes	**No**	**Remarks**
Is any maintenance schedule prepared?			
Is the maintenance of the system done in routine basis?			
Is support from the supplier ensured?			
Is maintenance book maintained?			
Is responsible personnel for maintenance identified?			
Log book of maintenance done on routine basis?			
Who is responsible for maintain the system?			
Is support and maintenance report generated monthly?			
Is warranty endured of the total system (hardware and software)?			

Training	**Review Outcome**		
	Yes	**No**	**Remarks**
Is need assessment of training done?			
Is trainee selection done with relevance to objective/ ICT component?			
Is type of training identified? (Basic / specialized ICT training)?			
Is trainer selection is done accordingly to qualification?			
Is training venue is properly equipped?			
Is training module is up to date?			
Is feedback on training given by participant?			
How training is comply with objective of project?			

Sustainability Plan and Human Resource	**Review Outcome**		
	Yes	**No**	**Remarks**
Is Exit Plan specified?			
Is Sustainability Plan specified?			
Are human resource being ensured to implement / monitor the ICT project component? (at the time of implementation and after implementation)			

ANNEXURE - 6
Checklist for Impact Evaluation of ICT Projects

1	Ministry/ Division	
2	Implementing Agency	
3	Project Name and ID	
4	Date of Commencement	
5	Expected Project Completion Date as per DPP/TPP	
6	Actual Date of Completion	
7	Original Budget	
8	Actual Expenditure	
9	Development Partner Name (if any)	
10	Brief Description of Project Components	
11	Major ICT Components	
12	Procurement Methods Used	
13	Project Time Overrun	• Less than 1 year • Less than 2 years • More than 2 years

Impact Evaluation	Review Outcome		
	Yes	No	Remarks
Is the projects outcome reflected the project objective?			
What are the main component of the project?			
Source of the fund of the project?			
Weather the component implemented is relevant with project objective?			
What was the physical progress of the project during project completion?			
Current usage of the implemented project component?			
Benefit cost ratio, Net Present Value and Internal rate of return are consistent between estimated value and actual return value?			
How sustainability of the project ensured?			

Who are the direct and indirect beneficiary of the project?			
Is there any social impact exists after completion of the project?			
Is there any economic impact exists after completion of the project?			
Is the project contributed to the Annual development programme and Strategic development goal?			
Is any support or maintenance provided by procuring entity?			
What is the performance of the system?			
Is there any technical person associated with for running the system or for maintenance?			
Whether all system design documents are maintained?			
Whether all system maintenance log book are maintained?			
Whether hardware inventory list is maintained?			
Is hardware or software performed as per specification?			
What are the measures taken to replace/ fix a faulty hardware?			
Is maintenance book maintained?			
Whether project completion report is done?			
Main problems observed in project implementation.			
Causes of the problem observed.			
Steps taken to solve the problem.			

ANNEXURE – 7
Checklist for ICT Project Requirement and Analysis Review

ICT Project Background Analysis **(Information about the general factors that affect the IT products and their requirements)**	**Review Outcome**		
	Yes	**No**	**Remarks**
Has the feasibility study been done?(specifying the target group, functionality)			
Is Feasibility study, Benchmarking study, Requirements Analysis, Project Planning, Evaluation of available products, Technological trials done?			
Function and purpose of the system is defined			
Does the IT component fulfil the objectives of the project			
Specify where system is to be used and by whom			
Specify networks and platforms involved			
Identify relation to other systems - state whether the system is independent, subsystem of a larger one or a replacement			
Identify functionality of the system at all levels			
Identify relationship to other projects (put project in context of others past, present or future)			
Identify the kind of applications, tools and techniques to be used			
Identify limitations of IT component of the project			
Provide background information to justify constraints			
Justify the sustainability of the project in regard of software and hardware and the need of stakeholders			
Identify the product lifecycle associated with user need			
Estimated time for delivery of product			
Risk identification and risk management is done			
Cost analysis of IT components is done			
Strategic plan for implementation is done			

Requirement Analysis	Review Outcome		
	Yes	No	Remarks
Are all significant consumers of scarce resources (memory, network bandwidth, processor capacity, etc.) identified, and is their anticipated resource consumption specified?			
User Group and total user number of IT component identified?			
Is the human resource identified to run the IT component?			
Have all quality attributes (characteristics) been properly specified (i.e. efficiency, flexibility, interoperability, maintainability, portability, reusability, usability, availability)			
Has full life cycle support been addressed, including maintenance?			
Have all dependencies on other systems been identified? (Applications or application interfaces, databases, communications subsystems, networking, etc.)			
Are user documentation and training requirements addressed?			
Has Software Requirement Specification done along with User Requirements analysis, Technical requirements, design description and format of Forms and GUI screen prints.			
If the contract delivers hardware, specify requirements for each item of equipment; (specify: type, number, functionality, standards, interfaces, performance, capacity, expansibility, reliability, availability, durability, maintainability, running cost limitations, operational requirements etc)			
Is Software requirement validation done			
Is there any default pay back if any vendor unable to deliver the product in estimated time			
All functional capabilities are documented.			
Reuse of existing software is fully described.			
All adaptation requirements identified (e.g., geographic parameters, platform variations are identified).			
Applicable timing, resource usage (e.g., CPU, memory, bandwidth),			

and associated system load requirements are identified.			
Applicable safety requirements are identified.			
Applicable security requirements are identified.			
Applicable design constraint requirements (e.g., object-oriented design, language, support environment) are identified.			
Applicable acceptance criteria (e.g., test, inspection, demonstration) are identified.			
Specify all modules and functions of IT component			
All diagrams are provided before software implementation			
Has the System Design Document (or Software Design Document) been completed for all sections up to and including Conceptual Design?			
Is the project in compliance with IT Infrastructure Standards?			
Is the project in compliance with National Enterprise Architecture?			
Is all module completed as per diagram?			
Is the software performing fully as estimated capacity as per requirement analysis?			
Is Support and maintenance log book maintained?			
What constrains are faced during implementation and steps taken to solve the constrains			

Hardware Requirement	**Review Outcome**		
	Yes	**No**	**Remarks**
Hardware requirement was prepared by an ICT personnel			
Whether hardware were procured as per specification			
Specify the specification of hardware with justification			
Specify the hardware lifecycle			
Specify technological barrier for users (if any)			
Define processor and its speed			
Determine amount of available memory needed			
Hard disk space requirements			
Determine if any display resolution issues exist			
Special peripheral devices (Printer, scanners, etc.)			
Training required			
Ongoing maintenance requirements			
Network access requirements			
Sufficient CPU utilization on existing hardware for both online and batch?			
Sufficient memory on existing hardware for both online and batch?			
Determine if need additional equipment			
Determine if need specialized hardware and/or component not already part of enterprise server farm			
Determine if need dedicated server resources			
Determine if estimated capacity requirements (CPU, memory, concurrent users, etc.) exceed existing available resources			
Determine if need specific type of disk storage (mirrored or RAID-5)			

Network checklist	**Review Outcome**		
	Yes	**No**	**Remarks**
Specify Network Infrastructure (the hardware that makes the network) with total unit used and used in network such as Data cabling, Switch / Hub gear, Routers, Firewalls, Patch cable management, Wireless access point(s), Antennas) with justification			
Specify network devices (the hardware that connects to the network) such as Servers, Workstation, Print Servers, Printers/ Copiers, Hand Held(s), PLC(s), IP Camera's, IP Phones etc used with justification			
Specify peripherals (the hardware that does not connect to the network) such as Local Printers, USB Hubs, Keyboards, Mice, Monitors / Displays, Hand Held, Removable storage devices, Digital Camera(s), Docking Station(s), Cell Phones used with justification			
Software to operate network such as Operating Systems, Productivity Applications, Support Applications, Device drivers, Services, Engines etc used with justification			
Administrative (Information that makes the large amount of computer equipment a valuable networked system) such as Users, Passwords, Groups, Login Scripts, Licenses, Policies used with justification			
Diagrams (The graphical representation of your network € Geographic outline of all organization locations / WAN diagram, Floor plan for each location, Data jack map, LAN diagram, Infrastructure map used with justification			
Is network is in function or generate the expected outcome			
Is the maintenance check up done in routine basis			
Log book of maintenance done on routine basis			

ANNEXURE – 8
Suggested Checklist for Data Center

Sl No	Issues	Remarks
1	For physical rooms and areas within the data center there is provision of Physical Site Layout.	
1.1	Is the data center located at a physically safe area?	
1.2	Has the data center been designed with ample space for expansion to meet the growing demands?	
1.3	Has the data center been implemented 24/7 physical security monitoring through CCTV Surveillance Monitoring (e.g. Closed-circuit television (CCTV) /Automated Security Intrusion Alarm/Biometric/Motion Detector)?	
1.4	Does the data center has standardize use of 19-inch 42U racks which aids better cabling management and for cold/ hot air aisle efficiency?	
1.5	Do all racks have perforated doors for front and back for front-in and back-out cross-air movement?	
1.6	Has client conducted a risk assessment before building or implementing a data center?	
1.7	Implement appropriate controls to mitigate identified risks.	
1.8	Is the location of disaster recovery site separated from the primary data center?	
1.9	Does is ensure smoke detection and fire suppression systems are in place and tested on periodic basis?	
1.10	Is it designed data center with ample space for growth?	
1.11	Is the data center located at a physically safe area?	
2	Cabling Infrastructure	
2.1	Backbone Cabling – Has Fibre Optic Cable (FOC) been used for backbone cabling?	
2.2	Horizontal Cabling –Has Category 6 been used for horizontal cabling?	
3	Environmental Factors	
3.1	Power/Cooling –Has client carried out a detailed capacity requirements study for space, power and cooling?	
3.2	Cooling – Does the data center implemented ‘hot’ and ‘cold’ aisle setup for effective cooling?	
3.2	Will the data center be hosted at Bangladesh Computer Council?	

ANNEXURE – 9

Checklist for Web Applications

Objective: Access to web content is implemented in a secure and accountable manner.

Checklist	**Remarks**
Agencies must develop and implement a policy governing appropriate Web usage.	
Agencies should use a Web proxy for all Web browsing activities.	
An agency's web proxy should authenticate system users and provide logging that includes at least the following details about websites accessed: ▪ address (uniform resource locator) ▪ time/date ▪ system user ▪ internal IP address ▪ external IP address	
Agencies should not permit downloading of executable files from external websites unless there is a demonstrable and approved business requirement.	
Agencies should disable the automatic launching of files downloaded from external websites.	
Agencies permitting SSL through their gateways should implement: ▪ a solution that decrypts and inspects the SSL traffic as per content filtering requirements ▪ a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked	
Agencies should implement whitelisting for all HTTP traffic being communicated through their gateways.	
Agencies using a whitelist on their gateways to specify the external addresses, to which encrypted connections are permitted, should specify whitelist addresses by domain name or IP address.	
If agencies do not whitelist websites, they should blacklist websites to prevent access to known malicious websites.	
Agencies blacklisting websites should update the blacklist on a frequent basis to ensure that it remains effective.	
Agencies should block client-side active content, such as Java and ActiveX, which are assessed as having a limited business impact.	
Agencies should: ▪ use client-side controls that allow JavaScript on a per website basis ▪ add JavaScript functions used only for malicious purposes to the agency Web content filter or IDS/IPS	
Agencies should use the Web proxy to filter content that is potentially harmful to system users and their workstations	
Users should not store web site authentication credentials (user ID and password) on workstations, remote access devices (such as laptops) or BYO8 devices	
Users should not use the same password for multiple websites	

ANNEXURE – 10
Checklist for Information Security Documentation

Objective: Information security documentation is produced for systems, to support and demonstrate good governance.

Checklist	Remarks
Agencies must have an Information Security Policy for their agency.	
Agencies must ensure that every system is covered by a Security Risk Management Plan	
Agencies must ensure that every system is covered by a Security Plan	
Agencies must ensure that Standard Operating Procedures (SOPs) are developed for systems	
Agencies must develop an Incident Response Plan and supporting procedures	
Agency personnel must be trained in, and exercise the Incident Response Plan	
Agencies must ensure that their Information Security Policy, Security Risk Management Plan, Security Plan, Standard Operating Procedures and Incident Response Plan are appropriately classified	
Agencies should create and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other	
Agencies should ensure that their security protocol and SOPs are logically connected and consistent for each system, other agency systems and with the agency's Security Plan.	
The security protocol should include an acceptable use policy for any agency technology equipment, systems, resources and data	
All information security documentation should be formally approved and signed off by a person with an appropriate level of seniority and authority	
Agencies should ensure that all high-level information security documentation is approved by the agency head or their delegate	
Agencies should ensure that all system-specific documents are reviewed by the system owner	
Agencies should develop a regular schedule for reviewing all information security documentation	
Agencies should ensure that information security documentation is reviewed at least annually with the date of the most recent review being recorded on each document	

ANNEXURE – 11
Checklist for Incident Response Plans

Objective: Incident Response Plans (IRP) outline actions to take in response to an information security incident

Checklist	Remarks
Agencies must include, as a minimum, the following content within their IRP: ▪ broad guidelines on what constitutes an information security incident ▪ the minimum level of information security incident response and investigation training for system users and system administrators ▪ the authority responsible for initiating investigations of an information security incident ▪ the steps necessary to ensure the integrity of evidence supporting an information security incident ▪ the steps necessary to ensure that critical systems remain operational ▪ when and how to formally report information security incidents ▪ National policy requirements for incident reporting.	
Agencies should include the following content within their IRP: ▪ clear definitions of the types of information security incidents that are likely to be encountered ▪ the expected response to each information security incident type ▪ the authority within the agency that is responsible for responding to information security incidents ▪ the criteria by which the responsible authority would initiate or request formal police investigations of an information security incident ▪ which other agencies or authorities need to be informed in the event of an investigation being undertaken ▪ the details of the system contingency measures or a reference to these details if they are located in a separate document	

ANNEXURE – 12
Checklist for Vulnerability Analysis

Objective: Exploitable information system weaknesses can be identified by vulnerability analysis and inform risks to systems

Checklist	Remarks
Agencies should implement a vulnerability analysis strategy by: ▪ monitoring public domain information about new vulnerabilities in operating systems and application software ▪ considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner ▪ running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented ▪ using security checklists for operating systems and common applications ▪ examining any significant incidents on the agency's systems	
Agencies should conduct vulnerability assessments in order to establish a baseline: ▪ before a system is first used ▪ after any significant incident ▪ after a significant change to the system ▪ after changes to standards, policies and guidelines	
Agencies should analyze and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment	

ANNEXURE – 13
Checklist for Business Continuity and Disaster Recovery

Objective: To ensure business continuity and disaster recovery processes are established to assist in meeting the agency's business requirements, minimize any disruption to the availability of information and systems, and assist recoverability

Checklist	Remarks
Agencies must determine availability and recovery requirements for their systems and implement appropriate measures to support them	
Agencies should: ▪ identify vital records ▪ backup all vital records ▪ store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the requirements ▪ test backup and restoration processes regularly to confirm their effectiveness	
Agencies should develop and document a business continuity plan	
Agencies should develop and document a disaster recovery plan	

ANNEXURE – 14
Checklist for Servers and Network Devices

Objective: Secured server and communications rooms provide appropriate physical security for servers and network devices

Checklist	Remarks
Agencies must ensure that servers and network devices are secured within cabinets as outlined by GoB	
Agencies must ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled	
Agencies must not leave server rooms, communications rooms or security containers in an unsecured state unless the server room is occupied by authorized personnel	
Agencies must develop a Site Security Plan (Site Plan) for each server and communications room. Information to be covered includes, but is not limited to: ▪ a summary of the security risk review for the facility the server or communications room is located in ▪ roles and responsibilities of facility and security personnel ▪ the administration, operation and maintenance of the electronic access control system or security alarm system ▪ key management, the enrolment and removal of system users and issuing of personal identification number codes and passwords ▪ regular inspection of the generated audit trails and logs ▪ end of day checks and lockup ▪ reporting of information security incidents ▪ what activities to undertake in response to security alarms	
Agencies should use a secured server or communications room within a secured facility	
Agencies should locate patch panels, fiber distribution panels and structured wiring enclosures within at least lockable commercial cabinets	
Agencies should use fiber optic cabling	
Cabling should be inspectable at a minimum of five-meter intervals	
Approved cable groups may share a common reticulation system but should have either a dividing partition or a visible gap between the differing cable groups or bundles	
Flexible or plastic conduit should be used in walls to run cabling from cable trays to wall outlets	
Approved cable groups should have either a dividing partition or a visible gap between the individual cable groups. If the partition or gap exists, cable groups may share a common reticulation system	
Cabling from cable trays to wall outlets should run in flexible or plastic conduit.	
Power filters should be used to provide a filtered power supply and reduce	

opportunity for technical attacks	
In a shared Non-Government Facility agencies should use fiber optic cabling	
Cabling should be inspectable at a minimum of five-meter intervals	
Flexible or plastic conduit should be used in walls to run cabling from cable trays to wall outlets	
The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings should be clear plastic or be inspectable and have tamper proof seals fitted	
Conduit joints should be sealed with glue or sealant	

ANNEXURE – 15

Checklist for Software Application Development

Objective: Secure programming methods and testing are used for application development in order to minimize the number of coding errors and security vulnerabilities

Checklist	Remarks
Agencies should ensure that software development environments are configured such that: ▪ there are at least three separate environments covering: o development o testing o production ▪ information flow between the environments is strictly limited according to a defined and documented policy, with access granted only to system users with a clear business requirement ▪ new development and modifications only take place in the development environment ▪ write access to the authoritative source for the software (source libraries & production environment) is disabled	
Agencies should ensure that software developers use secure programming practices when writing code, including: ▪ designing software to use the lowest privilege level needed to achieve its task ▪ denying access by default ▪ checking return values of all system calls ▪ validating all inputs	
Software should be reviewed or tested for vulnerabilities before it is used in a production environment	
Software should be reviewed or tested by an independent party as well as the developer	
Software development should follow secure coding practices and agency development standards	
Agencies should review all active content on their Web servers for known information security issues	
Agencies should minimize connectivity and access between each Web application component	
Agencies should follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services	

ANNEXURE – 16
Checklist for Access Control

Objective: Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems

Checklist	Remarks
Agencies must: ▪ develop and maintain a set of policies and procedures covering system users': ▪ identification ▪ authentication ▪ authorization ▪ make their system users aware of the agency's policies and procedures	
Agencies must ensure that all system users are: ▪ uniquely identifiable ▪ authenticated on each occasion that access is granted to a system	
If agencies choose to allow shared, non-user-specific accounts they must ensure that an independent means of determining the identification of the system user is implemented	
Agencies must not use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system	
Agencies must not allow storage of unprotected authentication information that grants system access, or decrypts an encrypted device, to be located on, or with the system or device, to which the authentication information grants access	
Agencies must ensure system users provide sufficient evidence to verify their identity when requesting a password reset for their system account	
Agencies should not use shared credentials to access accounts	
Agencies should ensure that they combine the use of multiple methods when identifying and authenticating system users	
Agencies should implement a password policy enforcing either: ▪ a minimum password length of 16 characters with no complexity requirement or ▪ a minimum password length of ten characters, consisting of at least three of the following character sets: ▪ lowercase characters (a-z) ▪ uppercase characters (A-Z) ▪ digits (0-9) ▪ punctuation and special characters	
Agencies should: ▪ ensure that passwords are changed at least every 90 days ▪ prevent system users from changing their password more than once a day	

▪ check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements ▪ force the system user to change an expired password on initial logon or if the password is reset	
Agencies should not: ▪ allow predictable reset passwords ▪ reuse passwords when resetting multiple accounts ▪ store passwords in the clear on the system ▪ allow passwords to be reused within eight password changes ▪ allow system users to use sequential passwords	
Agencies should disable LAN[13] Manager for password authentication on workstations and servers	
Agencies should develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity	
Agencies should: ▪ configure systems with a session or screen lock ▪ configure the lock to activate: ▪ after a maximum of 15 minutes of system user inactivity or ▪ if manually activated by the system user ▪ configure the lock to completely conceal all information on the screen ▪ ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated ▪ have the system user re-authenticate to unlock the system ▪ deny system users the ability to disable the locking mechanism	
Agencies should: ▪ lock system user accounts after three failed logon attempts ▪ have a system administrator reset locked accounts ▪ remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the agency ▪ remove or suspend inactive accounts after a specified number of days	
Agencies should have a logon banner that requires a system user to acknowledge and accept their security responsibilities before access to the system is granted	
Agency logon banners should cover issues such as: ▪ the system's description ▪ access only being permitted to authorized system users ▪ the system user's agreement to abide by relevant security policies ▪ the system user's awareness of the possibility that system usage is being monitored ▪ the definition of acceptable use for the system ▪ legal ramifications of violating the relevant policies	
Agencies should configure systems to display the date and time of the system user's previous login during the login process	
Agencies must have authorization of system users enforced by access	

controls	
Agencies must restrict access to compartmented information. Such restriction must be enforced by the system	
Only trusted personnel are granted privileged access to systems	
Agencies should: ▪ ensure strong change management practices are implemented ▪ ensure that the use of privileged accounts is controlled and accountable ▪ ensure that system administrators are assigned an individual account for the performance of their administration tasks ▪ keep privileged accounts to a minimum ▪ allow the use of privileged accounts for administrative work only	
Agencies must authenticate each remote connection and user prior to permitting access to an agency system	
Agencies should authenticate both the remote system user and device during the authentication process	
Agencies should not allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges	
Agencies should establish VPN connections for all remote access connections	
Agencies must develop and document logging requirements covering: ▪ the logging facility, including: ▪ log server availability requirements ▪ the reliable delivery of log information to the log server ▪ the list of events associated with a system or software ▪ component to be logged ▪ event log protection and archival requirements	
For each event identified as needing to be logged, agencies must ensure that the log facility records at least the following details, where applicable: ▪ date and time of the event ▪ relevant system user(s) or processes ▪ event description ▪ success or failure of the event ▪ event source (e.g. application name) ▪ IT equipment location/identification	
Event logs must be protected from: ▪ modification and unauthorised access ▪ whole or partial loss within the defined retention period	
Event logs must be archived and retained for an appropriate period as determined by the agency	
Disposal or archiving of DNS[14], proxy[15], event, systems and other operational logs must be in accordance with the provisions or the relevant legislation	
Agencies must develop and document event log audit requirements covering: ▪ the scope of audits	

▪ the audit schedule ▪ action to be taken when violations are detected ▪ reporting requirements ▪ roles and specific responsibilities	
Agencies should determine a policy for the retention of system management logs	
A system management log should record the following minimum information: ▪ all system start-up and shutdown service, application, component or system failures ▪ maintenance activities ▪ backup and archival activities ▪ system recovery activities ▪ special or out of hours' activities	
Agencies should log the events listed in the Annex 6 for specific software components	
Agencies should log, at minimum, the following events for all software components: ▪ user login ▪ all privileged operations ▪ failed attempts to elevate privileges ▪ security related system alerts and failures ▪ system user and group additions, deletions and modification to permissions ▪ unauthorized or failed access attempts to systems and files identified as critical to the agency	
Agencies should establish an authoritative time source	
Agencies should synchronize all logging and audit trails with the time source to allow accurate time stamping of events	
Agencies should ensure that: ▪ systems are configured to save event logs to a separate secure log server ▪ event log data is archived in a manner that maintains its integrity	
Agencies should retain DNS, proxy and event logs for at least 18 months.	

ANNEXURE – 17
Glossary

Access Point: A device that allows wireless-equipped computers and other devices to communicate with a wired network.

Accessibility: The process of designing and developing Web sites and other technology that can be navigated and understood by all people, including those with visual, hearing, motor, or cognitive impairments. This type of design also can benefit people with older/slower software and hardware.

ActiveX: A technology from Microsoft that links desktop applications to the World Wide Web. Using ActiveX tools, interactive web content can be created. Example: In addition to viewing Word and Excel documents from within a browser, additional functionality such as animation, credit card transactions, or spreadsheet calculations.

Address: Identifies the location of an Internet resource. Examples: an e-mail address (secretary@imed.gov.bd); a web address (http://www.imed.go.bd); or Internet address (192.168.100.1).

Alias: A short, easy to remember name created for use in place of a longer, more complicated name; commonly used in e-mail applications.

Anonymous FTP: Archive sites where Internet users can log in and download files and programs without a special username or password. Typically, you enter anonymous as a username and your e-mail address as a password.

Anti-Spam: To prevent e-mail spam, both end users and administrators of e-mail systems use various anti-spam techniques. Some of these techniques have been embedded in products, services and software to ease the burden on users and administrators. No one technique is a complete solution to the spam problem, and each has trade-offs between incorrectly rejecting legitimate e-mail vs. not rejecting all spam, and the associated costs in time and effort. Cloud-Based Anti-SPAM e-mail service eliminates the problem almost entirely.

Applet: A program capable of running on any computer regardless of the operating system. Many applets can be downloaded from various sites on the Internet.

Application: A program designed for a specific purpose, such as word processing or graphic design.

ASCII file: A file that can be opened and read by standard text editor programs (for example, Notepad or Simple Text) on almost any type of computer. Also referred to as "plain text files". Examples: documents saved in ASCII format within word processors like Microsoft Word or WordPerfect; e-mail messages created by a program like Outlook; or HTML files.

Attachment: A file that is sent along with an e-mail message.

Authentication: The process of identifying yourself and the verification that you're who you say you are. Computers where restricted information is stored may require you to enter your username and password to gain access.

Backbone: A term that is often used to describe the main network connections that comprise the Internet or other major network.

Bandwidth: A measurement of the amount of data that can be transmitted over a network at any given time. The higher the network's bandwidth, the greater the volume of data that can be transmitted.

BCP: Business Continuity Plan, or "BCP," is a set of documents, instructions, and procedures which enable a business to respond to accidents, disasters, emergencies, and/or threats without any stoppage or hindrance in its key operations. It is also called a business resumption plan, disaster recovery plan, or recovery plan.

BI: Business Intelligence - A recognized industry term for organizational analytics, including historical, current, and predictive views of business operations.

Binary file: A file that cannot be read by standard text editor programs like Notepad or Simple Text. Examples: documents created by applications such as Microsoft Word or WordPerfect or DOS files with the extension ".com" or ".exe".

Bit: A binary digit (either 0 or 1); it is the most basic unit of data that can be recognized and processed by a computer.

Blog: Refers to a weblog, a web page that contains journal-like entries and links that are updated daily for public viewing.

Bluetooth: A wireless networking technology that allows users to send voice and data from one electronic device to another via radio waves.

BMP: Bitmap file; a common image format on Windows computers. Files of this type usually have the suffix ".bmp" as part of their name.

Bookmark: A feature available in certain programs like Internet Explorer, Firefox, and Acrobat Reader; it is a shortcut you can use to get to a particular web page (IE and Firefox) or to a specified location within a document (PDF).

Boolean logic: A form of algebra in which all values are reduced to either true/false, yes/no, on/off, or 1/0.

Bounce: A term applied to an e-mail message when it is returned to you as undeliverable.

Bridge: A device used for connecting two Local Area Networks (LANs) or two segments of the same LAN; bridges forward packets without analyzing or re-routing them.

Broadband connection: A high-speed Internet connection; at present, cable modems and DSL (Digital Subscriber Lines) are the two technologies that are most commonly available to provide such access.

Browser: A program used to access World Wide Web pages. Examples: Firefox, Safari or Internet Explorer.

Buffer: On a multitasking system, a certain amount of RAM that is allocated as a temporary holding area so that the CPU can manipulate data before transferring it to a particular device.

Buffered: Data that is collected but not made immediately available. Compare to a language translator who listens to a whole statement before repeating what the speaker has said rather than providing a word-by-word translation. Example: Streaming media data viewable using a tool like Real Media Player is buffered.

Business continuity: Business continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, and help desk. Business Continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

Byte: A group of adjacent binary digits that a computer processes as a unit to form a character such as the letter "C". A byte consists of eight bits.

Cable modem: A special type of modem that connects to a local cable TV line to provide a continuous connection to the Internet. Like an analog modem, a cable modem is used to send and receive data, but the difference is that transfer speeds are much faster. A 56 Kbps modem can receive data at about 53 Kbps, while a cable modem can achieve about 1.5 Mbps (about 30 times faster). Cable modems attach to a 10Base-T Ethernet card inside your computer.

Cache: Refers to: 1) a region of computer memory where frequently accessed data can be stored for rapid access; or 2) a optional file on your hard drive where such data also can be stored. Examples: Internet Explorer and Firefox have options for defining both memory and disk cache. The act of storing data for fast retrieval is called "caching".

Captcha: A challenge-response test in the form of an image of distorted text the user must enter that to determine whether the user is human or an automated bot.

Case-sensitive: Generally applies to a data input field; a case-sensitive restriction means lower-case letters are not equivalent to the same letters in upper-case. Example: "data" is not recognized as being the same word as "Data" or "DATA".

CBT: Computer-Based Training; a type of training in which a student learns a particular application by using special programs on a computer. Sometimes referred to as "CAI" (Computer-Assisted Instruction) or "CBI" (Computer-Based Instruction), although these two terms may also be used to describe a computer program used to assist a teacher or trainer in classroom instruction.

CD-R drive: A type of disk drive that can create CD-ROMs and audio CDs. CD-R drives that feature multi session recording allow you to continue adding data to a compact disk which is very important if you plan on using the drive for backup.

CD-ROM: Compact Disk, Read Only Memory; a high-capacity secondary storage medium. Information contained on a CD is read-only. Special CD-ROM mastering equipment available in the OIT Multimedia Lab can be reserved for creating new CDs.

CD-RW, CD-R disk: A CD-RW disk allows you to write data onto it multiple times instead of just once (a CD-R disk). With a CD-R drive you can use a CD-RW disk just like a floppy or zip disk for backing up files, as well as for creating CD-ROMs and audio CDs.

CGI: Common Gateway Interface; a mechanism used by most web servers to process data received from a client browser (e.g., a user). CGI scripts contain the instructions that tell the web server what to do with the data.

Chat: Real-time communication between two or more users via networked-connected computers. After you enter a chat (or chat room), any user can type a message that will appear on the monitors of all the other participants.

Client: A program or computer that connects to and requests information from a server. Examples: Internet Explorer or Firefox. A client program also may be referred to as "client software" or "client-server software".

Client-server technology: Refers to a connection between networked computers in which the services of one computer (the server) are requested by the other (the client). Information obtained is then processed locally on the client computer.

Cloud: (See below): Common shorthand for a provided cloud computing service (or even an aggregation of all existing cloud services) is "The Cloud".

Cloud computing: A general term used to describe Internet services such as social networking services (e.g., Facebook and Twitter), online backup services, and applications that run within a Web browser. Could computing also include computer networks that are connected over the Internet for server redundancy or cluster computing purposes.

CMS: 'Content Management System' is the collection of procedures used to manage work flow in a collaborative environment. In a CMS, data can be defined as nearly anything: documents, movies, pictures, phone numbers, scientific data, and so forth. CMSs are frequently used for storing, controlling, revising, semantically enriching, and publishing documentation. Serving as a central repository, the CMS increases the version level of new updates to an already existing file. Version control is one of the primary advantages of a CMS.

Compress: The process of making a file smaller so that it will save disk space and transfer faster over a network. The most common compression utilities are Winrar for PC or compatible computers (.zip files) and or Stuffit (.sit files) for Macintosh computers.

Connect: A term that commonly refers to accessing a remote computer; also a message that appears at the point when two modems recognize each other.

Cookie: A small piece of information you may be asked to accept when connecting to certain servers via a web browser. It is used throughout your session as a means of identifying you. A cookie is specific to, and sent only to the server that generated it.

Courseware: Software designed specifically for use in a classroom or other educational setting.

CPU: Central processing unit; the part of a computer that oversees all operations and calculations.

CSP: Cloud Service Provider; a business model for providing cloud services.

CSS: Cascading Style Sheet; A set of rules that define how web pages are displayed using CSS, designers can create rules that define how page

Cursor: A special symbol that indicates where the next character you type on your screen will appear. You use your mouse or the arrow keys on your keyboard to move the cursor around on your screen.

Cyberspace: A term describing the world of computers and the society that uses them.

DaaS: Desktop-as-a-Service - Also called virtual desktop or hosted desktop services, it is the outsourcing of a virtual desktop infrastructure (VDI) to a third- party service provider.

Daemon: A special small program that performs a specific task; it may run all the time watching a system, or it can take action only when a task needs to be performed.

Example: If an e-mail message is returned to you as undeliverable, you may receive a message from the mailer daemon.

Database: A collection of information organized so that a computer application can quickly access selected information; it can be thought of as an electronic filing system. Traditional databases are organized by fields, records (a complete set of fields), and files (a collection of records). Alternatively, in a Hypertext database, any object (e.g., text, a picture, or a film) can be linked to any other object.

Data center: A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.

Decompress: Opposite of compressing a file; the process of restoring the file to its original size and format. The most common programs for decompressing files are Winrar for PC and compatible computers (.zip files) and Stuffit Expander (.sit files) for Macintosh computers.

Defragmentation: The process of rewriting parts of a file to contiguous sectors on a hard drive to increase the speed of access and retrieval.

Desktop: On computers like IBM PC or compatibles and Macintoshes, the backdrop where windows and icons for disks and applications reside.

DHCP: Dynamic Host Configuration Protocol; a protocol that lets a server on a local network assign temporary IP addresses to a computer or other network devices.

Dialog box: Sometimes referred to as a window; on a graphical user interface system, an enclosed area displayed by a program or process to prompt a user for entry of information in one or more boxes (fields).

Dial-Up Adapter: A network component within Windows that enables you to connect to a dial up server via a modem. Users running dial-up connections on Windows computers must have Dial-Up Adapter installed and properly configured.

Dial up connection: A connection from your computer that goes through a regular telephone line. You use special communications software to instruct your modem to dial a number to access another computer system or a network. May also be referred to as "dial up networking".

Digital asset Intellectual content which has been digitized and can be referenced or retrieved online; for example, PowerPoint slides, audio or video files, or files created in a word processing application, etc.

Digitize: Sometimes referred to as digital imaging; the act of translating an image, a sound, or a video clip into digital format for use on a computer. Also used to describe the process of converting coordinates on a map to x,y coordinates for input to a computer. All data a computer processes must be digitally encoded as a series of zeroes and ones.

DIMM: Dual In-line Memory Module; a small circuit board that can hold a group of memory chips. A DIMM is capable of transferring 64 bits instead of the 32 bits each SIMM can handle. Pentium processors require a 64-bit path to memory so SIMMs must be installed two at a time as opposed to one DIMM at a time.

Directory: An area on a disk that contains files or additional divisions called "subdirectories" or "folders". Using directories helps to keep files organized into separate categories, such as by application, type, or usage.

Disaster recovery: Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

Disaster recovery planning: Also referred to as "DRP". Please see above explanation.

Discussion group: Another term for an online newsgroup or forum.

Distance education: May also be referred to as "online learning" or "eLearning." A means of instruction that implies a course instructor and students are separated in space and perhaps, in time. Interaction may be synchronous (facilitated) or asynchronous (self-paced). Students can work with various course materials, or they may use tools like chat or discussion groups to collaborate on projects.

Distance learning: The goal of distance education; distance learning and distance education are often used interchangeably.

DNS: Domain Name System; a service for accessing a networked computer by name rather than by numerical, (IP) address.

Domain: Part of an Internet address. The network hierarchy consists of domains and subdomains. At the top are a number of major categories (e.g., com, edu, gov); next are domains within these categories (e.g., ohio-state); and then there are subdomains. The computer name is at the lowest level of the hierarchy.

Download: The process of transferring one or more files from a remote computer to your local computer. The opposite action is upload.

Dpi: Dots per inch; a measure of a printer's resolution. The higher the number, the better the print quality. A minimum of 300 dpi usually is required for professional quality printing.

DRaaS: Disaster Recovery as a Service; a service that helps recover data in the event of a server failure or natural disaster.

Drag and drop: The act of clicking on one icon and moving it on top of another icon to initiate a specific action. Example: Dragging a file on top of a folder to copy it to a new location.

DSL: Digital Subscriber Line; an always on broadband connection over standard phone lines.

DVD: Digital video disk; a type of compact disc that holds far more information than the CD-ROMs that are used for storing music files. A DVD can hold a minimum of 4.7 GB, enough for a full-length movie. MPEG-2 is used to compress video data for storage on a DVD. DVD drives are backward-compatible and can play CD-ROMs.

DVD-RW, DVD-R disk: A DVD-RW disk allows you to write data onto it multiple times instead of just once like on a DVD-R disk. A DVD disk can hold a minimum of 4.7GB which is enough to store a full-length movie. Other uses for DVDs include storage for multimedia presentations that include both sound and graphics.

EAP: Extensible Authentication Protocol; a general protocol for authentication that also supports multiple authentication methods.

EGA: Extended Graphics Adapter; a card (or board) usually found in older PCs that enables the monitor to display 640 pixels horizontally and 350 vertically.

E-Learning: Electronic learning; applies to a wide scope of processes including Web-based learning, computer-based instruction, virtual classrooms, and digital collaboration. Content may be delivered in a variety of ways including via the Internet, satellite broadcast, interactive TV, and DVD- or CD-ROMs.

E-mail: Electronic mail; the exchange of messages between users who have access to either the same system or who are connected via a network (often the Internet). If a user is not logged on when a new message arrives, it is stored for later retrieval.

E-mail archiving: Email archiving is typically a stand-alone IT application that integrates with an enterprise email server, such a Microsoft Exchange. In addition to simply accumulating email messages, these applications index and provide quick, searchable access to archived messages independent of the users of the system, using different technical methods of implementation. The reasons a company may opt to implement an email archiving solution include protection of mission critical data, record retention for regulatory requirements or litigation, and reducing production email server load.

Emoticon: A combination of keyboard characters meant to represent a facial expression. Frequently used in electronic communications to convey a particular meaning, much like tone of voice is used in spoken communications. Examples: the characters :-) for a smiley face or ;-) for a wink.

Emulation: Refers to the ability of a program or device to imitate another program or device; communications software often include terminal emulation drivers to enable you to log on to a mainframe. There also are programs that enable a Mac to function as a PC.

Encryption: The manipulation of data to prevent accurate interpretation by all but those for whom the data is intended.

EPS: Encapsulated PostScript; a graphics format that describes an image in the PostScript language.

Ethernet: A popular network technology that enables data to travel at 10 megabits per second. Campus microcomputers connected to a network have Ethernet cards installed that are attached to Ethernet cabling. An Ethernet connection is often referred to as a "direct connection" and is capable of providing data transmission speeds over 500 Kbps.

Ethernet card: An adapter card that fits into a computer and connects to Ethernet cabling; different types of adaptor cards fit specific computers. Microcomputers connected to the campus network have some type of Ethernet card installed. Example: computers in campus offices or in dorms rooms wired for ResNet. Also referred to as "Ethernet adapter".

Expansion card: Also referred to as an expansion board; a circuit board you can insert into a slot inside your computer to give it added functionality. A card can replace an existing one or may be added in an empty slot. Some examples include sound, graphics, USB, Firewire, and internal modem cards.

Extension: A suffix preceded by a period at the end of a filename; used to describe the file type. Example: On a Windows computer, the extension ".exe" represents an executable file.

Female connector: A cable connector that has holes and plugs into a port or interface to connect one device to another.

Field: A single piece of information within a database (e.g., an entry for name or address). Also refers to a specific area within a dialog box or a window where information can be entered.

File: A collection of data that has a name (called the filename). Almost all information on a computer is stored in some type of file. Examples: data file (contains data such as a group of records); executable file (contains a program or commands that are executable); text file (contains data that can be read using a standard text editor).

Filter: Refers to: 1) a program that has the function of translating data into a different format (e.g., a program used to import or export data or a particular file); 2) a pattern that prevents non-matching data from passing through (e.g., email filters); and 3) in paint programs and image editors, a special effect that can be applied to a bit map.

Firewall: A method of preventing unauthorized access to or from a particular network; firewalls can be implemented in both hardware and software, or both.

FireWire: A way to connect different pieces of equipment so they can quickly and easily share information. FireWire is very similar to USB. It preceded the development of USB when it was originally created in 1995 by Apple. FireWire devices are hot pluggable, which means they can be connected and disconnected any time, even with the power on. When a new FireWire device is connected to a computer, the operating system automatically detects it and prompts for the driver disk (thus the reference "plug-and play").

Flash drive: A small device that plugs into computer's USB port and functions as a portable hard drive.

Flash memory: A type of memory that retains information even after power is turned off; commonly used in memory cards and USB flash drives for storage and transfer of data between computers and other digital products.

Folder: An area on a hard disk that contains a related set of files or alternatively, the icon that represents a directory or subdirectory.

Font: A complete assortment of letters, numbers, and symbols of a specific size and design. There are hundreds of different fonts ranging from businesslike type styles to fonts composed only of special characters such as math symbols or miniature graphics.

Frames: A feature of some web browsers that enables a page to be displayed in separate scrollable windows..

Freeware: Copyrighted software available for downloading without charge; unlimited personal usage is permitted, but you cannot do anything else without express permission of the author. Contrast to shareware; copyrighted software which requires you to register and pay a small fee to the author if you decide to continue using a program you download.

Fragmentation: The scattering of parts of the same disk file over different areas of a disk; fragmentation occurs as files are deleted and new ones are added.

FTP: File Transfer Protocol; a method of exchanging files between computers via the Internet. A program like WS_FTP for IBM PC or compatibles or Fetch for Macintosh is required. Files can contain documents or programs and can be ASCII text or binary data.

GIF: Graphics Interchange Format; a format for a file that contains a graphic or a picture. Files of this type usually have the suffix ".gif" as part of their name. Many images seen on web pages are GIF files.

Gigabyte (Gig or GB): 1024 x 1024 x 1024 (2 to the 30th power) bytes; it's usually sufficient to think of a gigabyte as approximately one billion bytes or 1000 megabytes.

GPS: Global Positioning System; a collection of Earth-orbiting satellites. In a more common context, GPS actually refers to a GPS receiver which uses a mathematical principle called "trilateration" that can tell you exactly where you are on Earth at any moment.

Greyware: Greyware (or grayware) refers to a malicious software or code that is considered to fall in the "grey area" between normal software and a virus. Greyware is a term for which all other malicious or annoying software such as adware, spyware, trackware, and other malicious code and malicious shareware fall under.

GUI: Graphical user interface; a mouse-based system that contains icons, drop-down menus, and windows where you point and click to indicate what you want to do. All new Windows and Macintosh computers currently being sold utilize this technology.

Handshaking: The initial negotiation period immediately after a connection is established between two modems. This is when the modems agree about how the data will be transmitted (e.g., error correction, packet size, etc.). The set of rules they agree on is called the protocol.

Hard disk: A storage device that holds large amounts of data, usually in the range of hundreds to thousands of megabytes. Although usually internal to the computer, some types of hard disk devices are attached separately for use as supplemental disk space. "Hard disk" and "hard drive" often are used interchangeably but technically, hard drive refers to the mechanism that reads data from the disk.

Hardware: The physical components of a computer including the keyboard, monitor, disk drive, and internal chips and wiring. Hardware is the counterpart of software.

Header: The portion of an e-mail message or a network newsgroup posting that precedes the body of the message; it contains information like who the message is from, its subject, and the date. A header also is the portion of a packet that proceeds the actual data and contains additional information the receiver will need.

Help desk: A help desk is an information and assistance resource that troubleshoots problems with computers or similar products. Corporations often provide help desk support their employees and to their customers via a toll-free number, website and/or e-mail.

Helper application: A program used for viewing multimedia files that your web browser cannot handle internally; files using a helper application must be moved to your computer before being shown or played. Contrast to a plug-in which enables you to view the file over the Internet without first downloading it.

Home page: A document you access using a web browser like Firefox or Internet Explorer. It usually refers to the first page of a particular web site; it also is the page that automatically loads each time you start your browser.

Host: A computer accessed by a user working at a remote location. Also refers to a specific computer connected to a TCP/IP network like the Internet.

HTML: HyperText Markup Language; a language used for creating web pages. Various instructions and sets of tags are used to define how the document will look.

HTTP: HyperText Transfer Protocol; a set of instructions that defines how a web server and a browser should interact. Example: When you open a location (e.g., enter a URL) in your browser, what actually happens is an HTTP command is sent to the web server directing it to fetch and return the requested web page.

Hyperlink: Connects one piece of information (anchor) to a related piece of information (anchor) in an electronic document. Clicking on a hyperlink takes you to directly to the linked destination which can be within the same document or in an entirely different document. Hyperlinks are commonly found on web pages, word documents and PDF files.

Hypertext: Data that contains one or more links to other data; commonly seen in web pages and in online help files. Key words usually are underlined or highlighted. Example: If you look for information about "Cats" in a reference book and see a note that says "Refer also to Mammals" the two topics are considered to be linked. In a hypertext file, you click on a link to go directly to the related information.

Hypervisor: A hypervisor, also called virtual machine manager (VMM), is one of many hardware virtualization techniques that allow multiple operating systems, termed guests, to run concurrently on a host computer. It is so named because it is conceptually one level higher than a supervisory program. The hypervisor presents to the guest operating systems a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. Hypervisors are installed on server hardware whose only task is to run guest operating systems. Non-hypervisor virtualization systems are used for similar tasks on dedicated server hardware, but also commonly on desktop, portable and even handheld computers.

IaaS: Infrastructure as a Service; In the most basic cloud-service model, providers of IaaS offer computers - physical or (more often) virtual machines - and other resources.

icon: On a system like Windows or Macintosh that uses a graphical user interface (GUI), a small picture or symbol that represents some object or function. Examples: a file folder for a directory; a rectangle with a bent corner for a file; or a miniature illustration for a program.

ICS: Internet Connection Sharing; a feature in Windows that when enabled, allows you to connect computer on your home network to the Internet via one computer.

image map: A graphic overlay that contains more than one area (or hot spot) which is clickable and links to another web page or anchor. Image maps provide an alternative to text links for directing the user to additional information.

IMAP: Internet Message Access Protcol. A method of accessing e-mail messages on a server without downloading them to your local hard drive; it is the main difference between IMAP and POP3 which requires messages to be downloaded to a user's hard drive before the message can be read.

Internet: A worldwide network based on the TCP/IP protocol that can connect almost any make or model of popular computers from micros to supercomputers. Special programs called "clients" enable users with a network connection to do things like process e-mail or browse web sites using the familiar interface of a desktop computer.

Internet Explorer: A client program from Microsoft that comes pre installed on most new PC or compatible computers; enables you to browse the World Wide Web.

Internet radio: An audio broadcasting service transmitted via the Internet; broadcasts consist of a continuous stream. A drawback is the inability to control selection as you can when listening to traditional radio broadcasting.

IP address: Internet Protocol address; every computer connected to the Internet has a unique identifying number. Example: 192.168.100.2.

IRC: Internet Relay Chat; a system that enables two or more Internet users to conduct online discussions in real time.

IRQ: Interrupt request; refers to a number associated with a serial port on an PC or compatible computer. It usually can be changed by flipping a dip switch. Occasionally, when you're using a modem connect to the Internet, you may need to adjust the IRQ number assigned to the serial port which connects the modem to avoid conflicts with another device like your mouse.

ISP: Internet Service Provider; an organization or company that provides Internet connectivity.

IT Assessment: An IT Assessment is the practice of gathering information on part or whole of a IT network infrastructure, and then presented in a detailed report. This report typically analyzes the current state or health of technology or services and identifies areas needing improvement or prepare for a some type of system or application upgrade. IT Assessment can be performed in-house or outsourced to an IT vendor.

IV&V: Independent Verification and Validation (IV&V) is the process of checking that a project, service, or system meets specifications and that it fulfills its intended purpose. If you've recently implemented a new technology solution, you may want an independent party to assess the quality of the work.

Java: A general purpose programming language commonly used in conjunction with web pages that feature animation. Small Java applications are called Java applets; many can be downloaded and run on your computer by a Java-compatible browser like Firefox or Internet Explorer.

JavaScript: A publicly available scripting language that shares many of the features of Java; it is used to add dynamic content (various types of interactivity) to web pages.

JPEG: Joint Photographic Experts Group; a graphics format which compresses an image to save space. Most images imbedded in web pages are GIFs, but sometimes the JPEG format is used (especially for detailed graphics or photographs). In some cases, you can click on the image to display a larger version with better resolution.

Justified: A word processing format in which text is formatted flush with both the left and right margins. Other options include left justified (text is lined up against the left margin) and right justified (text is lined up against the right margin).

K: An abbreviation for kilobyte; it contains 1,024 bytes; in turn 1,024 kilobytes is equal to one megabyte.

Kbps: Kilobits per second; a measure of data transfer speed; one Kbps is 1,000 bits per second. Example: a 28.8 Kbps modem.

Kerberos: An authentication system developed at the Massachusetts Institute of Technology (MIT); it enables the exchange of private information across an open network by assigning a unique key called a "ticket" to a user requesting access to secure information.

Kerning: The amount of space between characters in a word; in desktop publishing, it is typically performed on pairs of letters or on a short range of text to fine-tune the character spacing.

Keyword: Most often refers to a feature of text editing and database management systems; a keyword is an index entry that correlates with a specific record or document.

Kilobyte (K, KB, or Kb): 1,024 (2 to the 10th power) bytes; often used to represent one thousand bytes. Example: a 720K diskette can hold approximately 720,000 bytes (or characters).

Knowledge base: A database where information common to a particular topic is stored online for easy reference; for example, a frequently-asked questions (FAQ) list may provide links to a knowledge base.

LAN: Local area network; a network that extends over a small area (usually within a square mile or less). Connects a group of computers for the purpose of sharing resources such as programs, documents, or printers. Shared files often are stored on a central file server.

Laser printer: A type of printer that produces exceptionally high quality copies. It works on the same principle as a photocopier, placing a black powder onto paper by using static charge on a rolling drum.

Leading: The vertical space between lines of text on a page; in desktop publishing, you can adjust the leading to make text easier to read.

Learning management system (LMS): Software used for developing, using, and storing course content of all types. Information within a learning management system often takes the form of learning objects (see "learning object" below).

Learning object: A chunk of course content that can be reused and independently maintained. Although each chunk is unique in its content and function, it must be able to communicate with learning systems using a standardized method not dependent on the system. Each chunk requires a description to facilitate search and retrieval.

Link: Another name for a hyperlink.

LINUX: An open-source operating system that runs on a number of hardware platforms including PCs and Macintoshes. Linux is freely available over the Internet.

List Processor: A program that manages electronic mailing lists; OIT is responsible for the List Processor software and also handles requests from the OSU community or new mailing lists.

LISTSERV, Listserver: An electronic mailing list; it provides a simple way of communicating with a large number of people very quickly by automating the distribution of electronic mail.

Log in, log on: The process of entering your username and password to gain access to a particular computer; e.g., a mainframe, a network or secure server, or another system capable of resource sharing.

MaaS: Metal-as-a-Service; The dynamic provisioning and deployment of whole physical servers, as opposed to the provisioning of virtual machines.

MAC: Media Access Control; The hardware address of a device connected to a shared network.

Macintosh: A personal computer introduced in the mid-1980s as an alternative to the IBM PC. Macintoshes popularized the graphical user interface and the 3 1/2 inch diskette drive.

Mail server: A networked computer dedicated to supporting electronic mail. You use a client program like Microsoft Outlook for retrieving new mail from the server and for composing and sending messages.

Mailing list: A collection of e-mail addresses identified by a single name; mailing lists provide a simple way of corresponding with a group of people with a common interest or bond. There are two main types of lists: 1) one you create within an e-mail program like Outlook that contains addresses for two or more individuals you frequently send the same message; and 2) a Listserve type that requires participants to be subscribed (e.g., a group of collaborators, a class of students, or often just individuals interested in discussing a particular topic).

Main memory: The amount of memory physically installed in your computer. Also referred to as "RAM".

Mainframe: A very large computer capable of supporting hundreds of users running a variety of different programs simultaneously. Often the distinction between small mainframes and minicomputers is vague and may depend on how the machine is marketed.

Male connector: A cable connector that has pins and plugs into a port or interface to connect one device to another.

malware: Software programs designed to damage or do other unwanted actions on a computer; common examples of malware include viruses, worms, trojan horses, and spyware.

Managed Workstations: A Managed Workstation reduces downtime, improves maintenance, increases productivity and data security through an effective blend of Help Desk and on-site support and centralized deployment of software patches and virus protection updates.

MAPI: Messaging Application Programming Interface; a system built into Microsoft Windows that enables different e-mail programs to interface to distribute e-mail. When both programs are MAPI-enabled, they can share messages.

MDM: Mobile Device Management; Any routine or tool intended to distribute applications, data, and configuration settings to mobile communications devices. The intent of MDM is to optimize the functionality and security of a mobile communications network. MDM must be part of a coherent BYOD strategy.

Megabyte (Meg or MB): 1,024 x 1,024 (2 to the 20th power) bytes; it's usually sufficient to think of a megabytes as one million bytes.

MHz or mHz: Megahertz; a measurement of a microprocessor's speed; one MHz represents one million cycles per second. The speed determines how many instructions per second a microprocessor can execute. The higher the megahertz, the faster the computer.

Menu: In a graphical user interface, a bar containing a set of titles that appears at the top of a window. Once you display the contents of a menu by clicking on its title, you can select any active command (e.g., one that appears in bold type and not in a lighter, gray type).

Microsoft Exchange: Microsoft Exchange Server is the server side of a client–server, collaborative application product developed by Microsoft. It is part of the Microsoft Servers line of server products and is used by enterprises using Microsoft infrastructure products. Exchange's major features consist of electronic mail, calendaring, contacts and tasks; support for mobile and web-based access to information; and support for data storage.

Microsoft Windows: A group of operating systems for PC or compatible computers; Windows provides a graphical user interface so you can point and click to indicate what you want to do.

MIME: Multipurpose Internet Mail Extensions; a protocol that enables you to include various types of files (text, audio, video, images, etc.) as an attachment to an e-mail message.

Modem: A device that enables a computer to send and receive information over a normal telephone line. Modems can either be external (a separate device) or internal (a board located inside the computer's case) and are available with a variety of features such as error correction and data compression.

Moderator: A person who reviews and has the authority to block messages posted to a supervised or "moderated" network newsgroup or online community.

Monitor: The part of a computer that contains the screen where messages to and from the central processing unit (CPU) are displayed. Monitors come in a variety of sizes and resolutions. The higher the number of pixels a screen is capable of displaying, the better the resolution. Sometimes may be referred to as a CRT.

Mouse: A handheld device used with a graphical user interface system. Common mouse actions include: 1) clicking the mouse button to select an object or to place the cursor at a certain point within a document; 2) double-clicking the mouse button to start a program or open a folder; and 3) dragging (holding down) the mouse button and moving the mouse to highlight a menu command or a selected bit of text.

MPEG: Motion Picture Experts Group; a high quality video format commonly used for files found on the Internet. Usually a special helper application is required to view MPEG files.

MRB: Managed Remote Back Up; a service that provides users with a system for the backup, storage, and recovery of data using cloud computing.

MSP: Managed Service Provider; A business model for providing information-technology services.

multimedia: The delivery of information, usually to a personal computer, in a combination of different formats including text, graphics, animation, audio, and video.

multitasking: The ability of a CPU to perform more than one operation at the same time; Windows and Macintosh computers are multitasking in that each program that is running uses the CPU only for as long as needed and then control switches to the next task.

NaaS: Network as a Service; a category of cloud services that provides users with the capability of where the capability provided to the cloud service user is to using network/transport connectivity services and/or inter-cloud network connectivity services.

nameserver: A computer that runs a program for converting Internet domain names into the corresponding IP addresses and vice versa.

NAT: Network Address Translation; a standard that enables a LAN to use a set of IP addresses for internal traffic and a single IP address for communications with the Internet.

Network: A group of interconnected computers capable of exchanging information. A network can be as few as several personal computers on a LAN or as large as the Internet, a worldwide network of computers.

Network adapter: A device that connects your computer to a network; also called an adapter card or network interface card.

Network hub: A common connection point for devices on a network.

NNTP: Network News Transport Protocol; the protocol used for posting, distributing, and retrieving network news messages.

Network monitoring: Cloud-based Network Monitoring service, can configure and remotely monitor all of your important network systems (e-mail, servers, routers, available disk space, backup applications, critical virus detection, and more). If our system detects a problem, it alerts Technical Support Center, so we can take corrective action. Depending on prearranged instructions from your own network engineers, we'll correct the problem immediately, wait until the next business day or simply notify you of the issue.

Network security: Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network Security is the authorization of access to data in a network, which is controlled by a network administrator. Every organization's needs are different and hackers are always adapting their techniques, so we are extremely serious about staying up to date with the latest network security tools, threats and industry developments.

OCR: Optical character recognition; the act of using a visual scanning device to read text from hard copy and translate it into a format a computer can access (e.g., an ASCII file). OCR systems include an optical scanner for reading text and sophisticated software for analyzing images.

on-Cloud: Businesses are moving more and more of their critical infrastructure to Cloud-based providers. 'On-Cloud' is currently our own term coined for providing management and support for your Cloud-based systems and processes.

on-site: At-place-of-work-or-business support, typically provided by a technically qualified individual.

online: A term that has commonly come to mean "connected to the Internet". It also is used to refer to materials stored on a computer (e.g., an online newsletter) or to a device like a printer that is ready to accept commands from a computer.

OpenType: OpenType is a format for scalable computer fonts. It was built on its predecessor TrueType, retaining TrueType's basic structure and adding many intricate data structures for prescribing typographic behavior. OpenType is a registered trademark of Microsoft Corporation.

PaaS: Platform as a Service, in the PaaS model, cloud providers deliver a computing platform that typically including an operating system, programming language execution environment, database, and web server.

Packet: A unit of transmission in data communications. The TCP/IP protocol breaks large data files into smaller chunks for sending over a network so that less data will have to be re-transmitted if errors occur.

Palette: The range of colors a computer or an application is able to display. Most newer computers can display as many as 16 million colors, but a given program may use only 256 of them. Also refers to a display box containing a set of related tools within a desktop publishing or graphics design program.

Page: Refers to an HTML document on the World Wide Web or to a particular web site; usually pages contain links to related documents (or pages).

Parallel port: An interface on a computer that supports transmission of multiple bits at the same time; almost exclusively used for connecting a printer. On IBM or compatible computers, the parallel port uses a 25-pin connector. Macintoshes have an SCSI port that is parallel, but more flexible in the type of devices it can support.

Password: A secret combination of characters used to access a secured resource such as a computer, a program, a directory, or a file; often used in conjunction with a username.

PC: Usually refers to an IBM PC or compatible, or when used generically, to a "personal computer". In a different context, PC also is an abbreviation for "politically correct."

PDA: Personal Digital Assistant; a small hand-held computer that in the most basic form, allows you to store names and addresses, prepare to-do lists, schedule appointments, keep track of projects, track expenditures, take notes, and do calculations. Depending on the model, you also may be able to send or receive e-mail; do word processing; play MP3 music files; get news, entertainment and stock quotes from the Internet; play video games; and have an integrated digital camera or GPS receiver.

PDF: Portable Document Format; a type of formatting that enables files to be viewed on a variety computers regardless of the program originally used to create them. PDF files retain the "look and feel" of the original document with special formatting, graphics, and color intact. You use a special program or print driver (Adobe Distiller or PDF Writer) to convert a file into PDF format.

Peer-to-peer: A type of connection between two computers; both perform computations, store data, and make requests from each other (unlike a client-server connection where one computer makes a request and the other computer responds with information).

Perl: Practical Extraction and Report Language; a programming language that is commonly used for writing CGI scripts used by most servers to process data received from a client browser.

Personality: A method of setting up a computer or a program for multiple users. Example: In Windows, each user is given a separate "personality" and set of relevant files.

Phishing: A con that scammers use to electronically collect personal information from unsuspecting users. Phishers send e-mails that appear to come from legitimate websites such as eBay, PayPal, or other banking institutions asking you to click on a link included in the email and then update or validate your information by entering your username and password and often even more information, such as your full name, address, phone number, social security number, and credit card number.

PING: Packet Internet Groper; a utility used to determine whether a particular computer is currently connected to the Internet. It works by sending a packet to the specified IP address and waiting for a reply.

pixel: Stands for one picture element (one dot on a computer monitor); commonly used as a unit of measurement.

plug-in: A program used for viewing multimedia files that your web browser cannot handle internally; files using a plug-in do not need to be moved to your computer before being shown or played. Contrast to a helper application which requires the file to first be moved to your computer. Examples of plug-ins: Adobe Flash Player (for video and animation) and Quicktime (for streamed files over the Internet).

plug and play: A set of specifications that allows a computer to automatically detect and configure a device and install the appropriate device drivers.

POP: Post Office Protocol; a method of handling incoming electronic mail. Example: E-mail programs may use this protocol for storing your incoming messages on a special cluster of servers called pop.service.ohio-state.edu and delivering them when requested.

pop-up blocker: Any application that disables the pop-up, pop-over, or pop-under ad windows that appear when you use a web browser.

post: The act of sending a message to a particular network newsgroup.

PostScript: A page description language primarily used for printing documents on laser printers; it is the standard for desktop publishing because it takes advantage of high resolution output devices. Example: A graphic design saved in PostScript format looks much better when printed on a 600 dpi printer than on a 300 dpi printer.

PostScript fonts: Called outline or scalable fonts; with a single typeface definition, a PostScript printer can produce many other fonts. Contrast to non-PostScript printers that represent fonts with bitmaps and require a complete set for each font size.

PPP: Point-to-Point Protocol; a type of connection over telephone lines that gives you the functionality of a direct Ethernet connection.

Program: A set of instructions that tells a computer how to perform a specific task.

Private cloud: Private cloud (also called internal cloud or corporate cloud) is a term for a proprietary computing architecture that provides hosted services to a limited number of users behind a secure and robust infrastructure. A private cloud solution is designed to offer the same features and benefits of shared cloud systems, but removes a number of objections to the cloud computing model including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

Protocol: A set of rules that regulate how computers exchange information. Example: error checking for file transfers or POP for handling electronic mail.

Proxy: Refers to a special kind of server that functions as an intermediate link between a client application (like a web browser) and a real server. The proxy server intercepts requests for information from the real server and whenever possible, fills the request. When it is unable to do so, the request is forwarded to the real server.

Public domain software: Any non-copyrighted program; this software is free and can be used without restriction. Often confused with "freeware" (free software that is copyrighted by the author).

Pull: Frequently used to describe data sent over the Internet; the act of requesting data from another computer. Example: using your web browser to access a specific page. Contrast to "push" technology when data is sent to you without a specific request being made.

Push: Frequently used to describe data sent over the Internet; the act of sending data to a client computer without the client requesting it. Example: a subscriptions service that delivers customized news to your desktop. Contrast to browsing the World Wide Web which is based on "pull" technology; you must request a web page before it is sent to your computer.

QoS: Quality of service; is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.

QuickTime: A video format developed by Apple Computer commonly used for files found on the Internet; an alternative to MPEG. A special viewer program available for both IBM PC and compatibles and Macintosh computers is required for playback.

RAM: Random Access Memory; the amount of memory available for use by programs on a computer. Also referred to as "main memory". Example: A computer with 8 MB RAM has approximately 8 million bytes of memory available. Contrast to ROM (read-only memory) that is used to store programs that start your computer and do diagnostics.

Record: A set of fields that contain related information; in database type systems, groups of similar records are stored in files. Example: a personnel file that contains employment information.

Registry: A database used by Windows for storing configuration information. Most 32-bit Windows applications write data to the registry. Although you can edit the registry, this is not recommended unless absolutely necessary because errors could disable your computer.

Remote backup: A remote, online, or managed backup service is a service that provides users with a system for the backup and storage of computer files. Remote backup solution incorporates automatic data compression and secure data encryption. This means that your critical system data backs up safely and efficiently.

Remote desktop: A Windows feature that allows you to have access to a Windows session from another computer in a different location (XP and later).

Remote login: An interactive connection from your desktop computer over a network or telephone lines to a computer in another location (remote site).

RGB: Red, green, and blue; the primary colors that are mixed to display the color of pixels on a computer monitor. Every color of emitted light can be created by combining these three colors in varying levels.

RJ-45 connector: An eight-wire connector used for connecting a computer to a local-area network. May also be referred to as an Ethernet connector.

ROM: Read Only Memory; a special type of memory used to store programs that start a computer and do diagnostics. Data stored in ROM can only be read and cannot be removed even when your computer is turned off. Most personal computers have only a few thousand bytes of ROM. Contrast to RAM (random access or main memory) which is the amount of memory available for use by programs on your computer.

Router: A device used for connecting two Local Area Networks (LANs); routers can filter packets and forward them according to a specified set of criteria.

RTF: Rich Text Format; a type of document formatting that enables special characteristics like fonts and margins to be included within an ASCII file. May be used when a document must be shared among users with different kinds of computers (e.g., IBM PC or compatibles and Macintoshes).

SaaS: Software as a Service; a software delivery model in which software and associated data are centrally hosted on the cloud. SaaS is typically accessed by users using a thin client via a web browser.

safe mode: A way of starting your Windows computer that can help you diagnose problems; access is provided only to basic files and drivers.

SAN: A storage area network (SAN) is a dedicated storage network that provides access to consolidated, block level storage. SANs primarily are used to make storage devices (such as disk arrays, tape libraries, and optical jukeboxes) accessible to servers so that the devices appear as locally attached to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the regular network by regular devices.

SATA: Serial Advanced Technology Attachment or Serial ATA. An interface used to connect ATA hard drives to a computer's motherboard that provides a better, more efficient interface; Serial ATA is likely to replace the previous standard, Parallel ATA (PATA), which has become dated.

Satellite transmission: A method of data transmission; the sender beams data up to an orbiting satellite and the satellite beams the data back down to the receiver.

screen reader: A software program that translates text on a Web page into audio output; typically used by individuals with vision impairment.

scroll bar: n a graphical user interface system, the narrow rectangular bar at the far right of windows or dialog boxes. Clicking on the up or down arrow enables you to move up and down through a document; a movable square indicates your location in the document. Certain applications also feature a scroll bar along the bottom of a window that can be used to move from side-to-side.

search engine: A tool that searches documents by keyword and returns a list of possible matches; most often used in reference to programs such as Google that are used by your web browser to search the Internet for a particular topic.

secure server: A special type of file server that requires authentication (e.g., entry a valid username and password) before access is granted.

security token: A small device used to provide an additional level of authorization to access a particular network service; the token itself may be embedded in some type of object like a key fob or on a smart card.

Self-extracting file: A type of compressed file that you can execute (e.g., double-click on the filename) to begin the decompression process; no other decompression utility is required. Example: on IBM PC or compatibles, certain files with an ".exe" extension and on Macintoshes, all files with a ".sea" extension.

Serial port: An interface on a computer that supports transmission of a single bit at a time; can be used for connecting almost any type of external device including a mouse, a modem, or a printer.

Server: A computer that is responsible for responding to requests made by a client program (e.g., a web browser or an e-mail program) or computer.

Shareware: Copyrighted software available for downloading on a free, limited trial basis; if you decide to use the software, you're expected to register and pay a small fee. By doing this, you become eligible for assistance and updates from the author. Contrast to public domain software which is not copyrighted or to freeware which is copyrighted but requires no usage fee.

signature: A file containing a bit of personal information that you can set to be automatically appended to your outgoing e-mail messages; many network newsreaders also have this capability. Large signatures over five lines generally are frowned upon.

SIMM: Single In-line Memory Module; a small circuit board that can hold a group of memory chips; used to increase your computer's RAM in increments of 1,2, 4, or 16 MB.

SMTP: Simple Mail Transfer Protocol; a method of handling outgoing electronic mail.

software: Any program that performs a specific function. Examples: word processing, spreadsheet calculations, or electronic mail.

spam: Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of spam that involves nearly identical messages sent to numerous recipients by email. Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. Spammers collect email addresses from chatrooms, websites, customer lists, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. They also use a practice known as “email appending” or "epending" in which they use known information about their target (such as a postal address) to search for the target's email address. Also see "Anti-Spam".

SSID: Service Set Identifier; a name that identifies a wireless network.

Streaming: A technique for transferring data over the Internet so that a client browser or plug-in can start displaying it before the entire file has been received; used in conjunction with sound and pictures. Example: The Flash Player plug-in from Adobe Systems gives your computer the capability for streaming audio; RealPlayer is used for viewing sound and video.

Spyware: Any software that covertly gathers user information, usually for advertising purposes, through the user's Internet connection.

subdirectory: An area on a hard disk that contains a related set of files; on IBM PC or compatibles, a level below another directory. On Macintoshes, subdirectories are referred to as folders.

SVGA: Super VGA (Video Graphics Array); a set of graphics standards for a computer monitor that offers greater resolution than VGA. There are several different levels including 800 x 600 pixels, 1024 by 768 pixels, 1280 by 1024 pixels; and 1600 by 1200 pixels. Although each supports a palette of 16 million colors, the number of simultaneous colors is dependent on the amount of video memory installed in the computer.

T-1 carrier: A dedicated phone connection supporting data rates of 1.544Mbits per second; T-1 lines are a popular leased line option for businesses connecting to the Internet and for Internet Service Providers connecting to the Internet backbone.

T-3 carrier: A dedicated phone connection supporting data rates of about 43 Mbps; T-3 lines are used mainly by Internet Service Providers connecting to the Internet backbone and for the backbone itself.

10Base-T: An adaptation of the Ethernet standard for Local Area Networks that refers to running Ethernet over twisted pair wires.

table: With reference to web design, a method for formatting information on a page. Use of tables and the cells within also provide a way to create columns of text. Use of tables vs frames is recommended for helping to make your web site ADA-compliant.

TCP/IP: Transmission Control Protocol/Internet Protocol; an agreed upon set of rules that tells computers how to exchange information over the Internet. Other Internet protocols like FTP, Gopher, and HTTP sit on top of TCP/IP.

Telephony: Telephony encompasses the general use of equipment to provide voice communication over distances, specifically by connecting telephones to each other.

Telnet: A generic term that refers to the process of opening a remote interactive login session regardless of the type of computer you're connecting to.

Terminal emulation: The act of using your desktop computer to communicate with another computer like a UNIX or IBM mainframe exactly as if you were sitting in front of a terminal directly connected to the system. Also refers to the software used for terminal emulation.

TIFF: Tag Image File Format; a popular file format for storing bit-mapped graphic images on desktop computers. The graphic can be any resolution and can be black and white, gray-scale, or color. Files of this type usually have the suffix ".tif" as part of their name.

Token: A group of bits transferred between computers on a token-ring network. Whichever computer has the token can send data to the other systems on the network which ensures only one computer can send data at a time. A token may also refer to a network security card, also known as a hard token.

Tool bar: On a graphical user interface system, a bar near the top of an application window that provides easy access to frequently used options.

Trojan horse: A harmless-looking program designed to trick you into thinking it is something you want, but which performs harmful acts when it runs.

TrueType: A technology for outline fonts that is built into all Windows and Macintosh operating systems. Outline fonts are scalable enabling a display device to generate a character at any size based on a geometrical description.

Tweet: An update of 140 characters or less published by a Twitter user meant to answer the question, "What are you doing?" which provides other users with information about you.

Twitter: A service that allows users to stay connected with each other by posting updates, or "tweets," using a computer or cell phone or by viewing updates posted by other users.

twisted pair cable: A type of cable that is typically found in telephone jacks; two wires are independently insulated and are twisted around each other. The cable is thinner and more flexible than the coaxial cable used in conjunction with 10Base-2 or 10Base-5 standards.

Two-factor authentication: An extra level of security achieved using a security token device; users have a personal identification number (PIN) that identifies them as the owner of a particular token. The token displays a number which is entered following the PIN number to uniquely identify the owner to a particular network service. The identification number for each user is changed frequently, usually every few minutes.

UNIX: A popular multitasking computer system often used as a server for electronic mail or for a web site. UNIX also is the leading operating system for workstations, although increasingly there is competition from Windows NT which offers many of the same features while running on an PC or compatible computer.

upload: The process of transferring one or more files from your local computer to a remote computer. The opposite action is download.

USB: Universal Serial Bus; a connector on the back of almost any new computer that allows you to quickly and easily attach external devices such as mice, joysticks or flight yokes, printers, scanners, modems, speakers, digital cameras or webcams, or external storage devices. Current operating systems for Windows and Macintosh computers support USB, so it's simple to install the device drivers. When a new device is connected, the operating system automatically activates it and begins communicating. USB devices can be connected or disconnected at any time.

username: A name used in conjunction with a password to gain access to a computer system or a network service.

URL: Uniform Resource Locator; a means of identifying resources on the Internet. A full URL consists of three parts: the protocol (e.g., FTP, gopher, http, nntp, telnet); the server name and address; and the item's path. The protocol describes the type of item and is always followed by a colon (:). The server name and address identifies the computer where the information is stored and is preceded by two slashes (//). The path shows where an item is stored on the server and what the file is called; each segment of the location s preceded by a single slash (/). Examples: The URL for the IMED home page is http://www.imed.gov.bd.

USB port: An interface used for connecting a Universal Serial Bus (USB) device to computer; these ports support plug and play.

utility: Commonly refers to a program used for managing system resources such as disk drives, printers, and other devices; utilities sometimes are installed as memory-resident programs. Example: the suite of programs called Norton Utilities for disk copying, backups, etc.

uuencode: A method of converting files into an ASCII format that can be transmitted over the Internet; it is a universal protocol for transferring files between different platforms like UNIX, Windows, and Macintosh and is especially popular for sending e-mail attachments.

VDI: Virtual Desktop Infrastructure or "VDI," is a desktop-centric service that hosts users' desktop environments on remote servers and/or blade PCs, which are accessed over a network using a remote display protocol.

virtual classroom: An online environment where students can have access to learning tools any time. Interaction between the instructor and the class participants can be via e-mail, chat, discussion group, etc.

virtualization: Virtualization is the creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system, a storage device or network resources. In hardware virtualization, the term host machine refers to the actual machine on which the virtualization takes place; the term guest machine, however, refers to the virtual machine. Likewise, the adjectives host and guest are used to help distinguish the software that runs on the actual machine from the software that runs on the virtual machine. The software or firmware that creates a virtual machine on the host hardware is called a hypervisor or Virtual Machine Monitor.

Virtual classroom: An online environment where students can have access to learning tools any time. Interaction between the instructor and the class participants can be via e-mail, chat, discussion group, etc.

Virtual hosting: Virtual hosting is a method for hosting multiple domain names on a computer using a single IP address. This allows one machine to share its resources, such as memory and processor cycles, to use its resources more efficiently.

Virtual memory: A technique that enables a certain portion of hard disk space to be used as auxiliary memory so that your computer can access larger amounts of data than its main memory can hold at one time.

Virtual reality: An artificial environment created with computer hardware and software to simulate the look and feel of a real environment. A user wears earphones, a special pair of gloves, and goggles that create a 3D display. Examples: manipulating imaginary 3D objects by "grabbing" them, taking a tour of a "virtual" building, or playing an interactive game.

Virus: A program intended to alter data on a computer in an invisible fashion, usually for mischievous or destructive purposes. Viruses are often transferred across the Internet as well as by infected diskettes and can affect almost every type of computer. Special antivirus programs are used to detect and eliminate them.

VoIP: Voice over Internet Protocol; a means of using the Internet as the transmission medium for phone calls. An advantage is you do not incur any additional surcharges beyond the cost of your Internet access.

VPN: Virtual Private Networking; a means of securely accessing resources on a network by connecting to a remote access server through the Internet or other network.

VT100: A type of terminal emulation required when you open an interactive network connection (telnet) to a UNIX system from your desktop computer.

WAIS: Wide Area Information Server; a program for finding documents on the Internet. Usually found on gopher servers to enable searching text-based documents for a particular keyword.

WAN: Wide Area Network; a group of networked computers covering a large geographical area (e.g., the Internet).

WAP: Wireless Application Protocol; a set of communication protocols for enabling wireless access to the Internet.

WEP: Wired Equivalent Privacy; a security protocol for wireless local area networks. WEP provides the same level of security as that of a wired LAN.

wi-fi: Wireless Fidelity; A generic term from the Wi-Fi Alliance that refers to of any type of 802.11 network (e.g., 802.11b, 802.11a, dual-band, etc.). Products approved as "Wi-Fi Certified" (a registered trademark) are certified as interoperable with each other for wireless communications.

Wild card: A special character provided by an operating system or a particular program that is used to identify a group of files or directories with a similar characteristic. Useful if you want to perform the same operation simultaneously on more than one file. Example: the asterisk (*) that can be used in DOS to specify a groups of files such as *.txt.

Window: On a graphical user interface system, a rectangular area on a display screen. Windows are particularly useful on multitasking systems which allow you to perform a number of different tasks simultaneously. Each task has its own window which you can click on to make it the current process. Contrast to a "dialog box" which is used to respond to prompts for input from an application.

Windows: A casual way of referring to the Microsoft Windows operating systems.

wireless (networking): The ability to access the Internet without a physical network connection. Devices such as cell phones and PDAs that allow you to send and receive e-mail use a wireless Internet connection based on a protocol called WAP (Wireless Application Protocol). At this point, web sites that contain wireless Internet content are limited, but will multiply as the use of devices relying on WAP increases.

Wizard: A special utility within some applications that is designed to help you perform a particular task. Example: the wizard in Microsoft Word that can guide you through creating a new document.

WLAN: Wireless Local Area Network; the computers and devices that make up a wireless network.

workstation: A graphical user interface (GUI) computer with computing power somewhere between a personal computer and a minicomputer (although sometimes the distinction is rather fuzzy). Workstations are useful for development and for applications that require a moderate amount of computing power and relatively high quality graphics capabilities.

World Wide Web: A hypertext-based system of servers on the Internet. Hypertext is data that contains one or more links to other data; a link can point to many different types of resources including text, graphics, sound, animated files, a network newsgroup, a telnet session, an FTP session, or another web server. You use a special program called a "browser" (e.g., Firefox or Internet Explorer) for viewing World Wide Web pages. Also referred to as "WWW" or "the web".

Worm: A program that makes copies of itself and can spread outside your operating system worms can damage computer data and security in much the same way as viruses.

WPA: Wi-Fi Protected Access; a standard designed to improve on the security features of WEP.

WWW: An abbreviation for World Wide Web.

WYSIWYG: What You See Is What You Get; a kind of word processor that does formatting so that printed output looks identical to what appears on your screen.

X2: A technology that enables data transmission speeds up to 56 Kbps using regular telephone service that is connected to switching stations by high-speed digital lines. This technology affects only transmissions coming into your computer, not to data you send out. In addition, your ISP must have a modem at the other end that supports X2.

XHTML: Extensible Hypertext Markup Language. A spinoff of the hypertext markup language (HTML) used for creating Web pages. It is based on the HTML 4.0 syntax, but has been modified to follow the guidelines of XML and is sometimes referred to as HTML 5.0.

XML: Extensible Markup Language; A markup language for coding web documents that allows designers to create their own customized tags for structuring a page.

zero-day: zero-day (or zero-hour or day zero) attack, threat or virus is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or the software developer, also called zero-day vulnerabilities. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability.

Zip: A common file compression format for PC or compatibles; the utility WinZip or Winrar is used for compressing and decompressing files. Zipped files usually end with a ".zip" file extension. A special kind of zipped file is self-extracting and ends with a ".exe" extension. Macintosh OSX also supports the .zip format and has tools that can compress and decompress zip files.

Zip drive: A high capacity floppy disk drive from Iomega Corporation; the disks it uses are a little bit larger than a conventional diskette and are capable of holding 100 MB or 250 MB of data.

Zoom: The act of enlarging a portion of an onscreen image for fine detail work; most graphics programs have this capability.

ANNEXURE – 18

References

- Cyber Security Strategy, 2014, BCC
- https://cptu.gov.bd/
- https://ictd.gov.bd/
- https://imed.gov.bd/
- https://nda.bcc.gov.bd/pages/standards.php
- https://www.bcc.gov.bd
- Guideline for Following Public Procurement Rules, Mohammad Mesbahuddin, Former Chief, Planning Commission, Bangladesh, 2014
- Information Security Manual, 2017, BCC
- National Digital Architecture, BCC
- National ICT Policy 2018, Bangladesh
- Public Email Policy 2018, Bangladesh
- SDG, 7FYP & ICT Policy by DoICT, Bangladesh