भारतीय प्रतिस्पर्धा आयोग
Competition Commission of India

REQUEST FOR PROPOSAL
Volume II

FOR

SELECTION OF
IT IMPLEMENTATION AGENCY

RFP No.	Date and Time
Last Date and Time for Submission of Proposals	18th March 2014 upto1500 hrs.
Date and Time of Opening of Technical Proposals	18th March 2014 at 1600 hrs.

COMPETITION COMMISSION OF INDIA
Hindustan Times House,
18-20, Kasturba Gandhi Marg,
New Delhi-110001
Tel: +91 11 23473400
Fax No: +91 11 23704686

Table of Contents

1. Introduction

The business processes of CCI are largely supported by the use of paper documents and folders passed from table to table and function to function.

CCI has proposed to leverage strength of information technology for bringing about efficiency in all its functions and processes, effectiveness in decision making and transparency in citizen centric interactions.

The following software applications identified by CCI should be COTS solutions which shall be implemented in two phases as under:

I. Phase I
   1. Document Management System and Workflow
   2. RFID Tracking Application
   3. Portal
   4. Website
   5. Identity & Access Management and System Security
   6. Data Leak/Loss Prevention Solution
   7. Management Information System
   8. Email and Messaging
   9. Human Resource Management System and Payroll
   10. Front Office Management System
   11. RFID based Library Management System
   12. Forensic Analysis Software
   13. Inventory and Asset Management
   14. Finance and Accounts Software
   15. Seminar and Event Management

II. Phase II
   1. Business Intelligence and Business Analytics
   2. Knowledge Management System
   3. Electronic Record Management System
   4. E-Discovery
   5. Audio/Video Conferencing

2. Solution and Technology Architecture

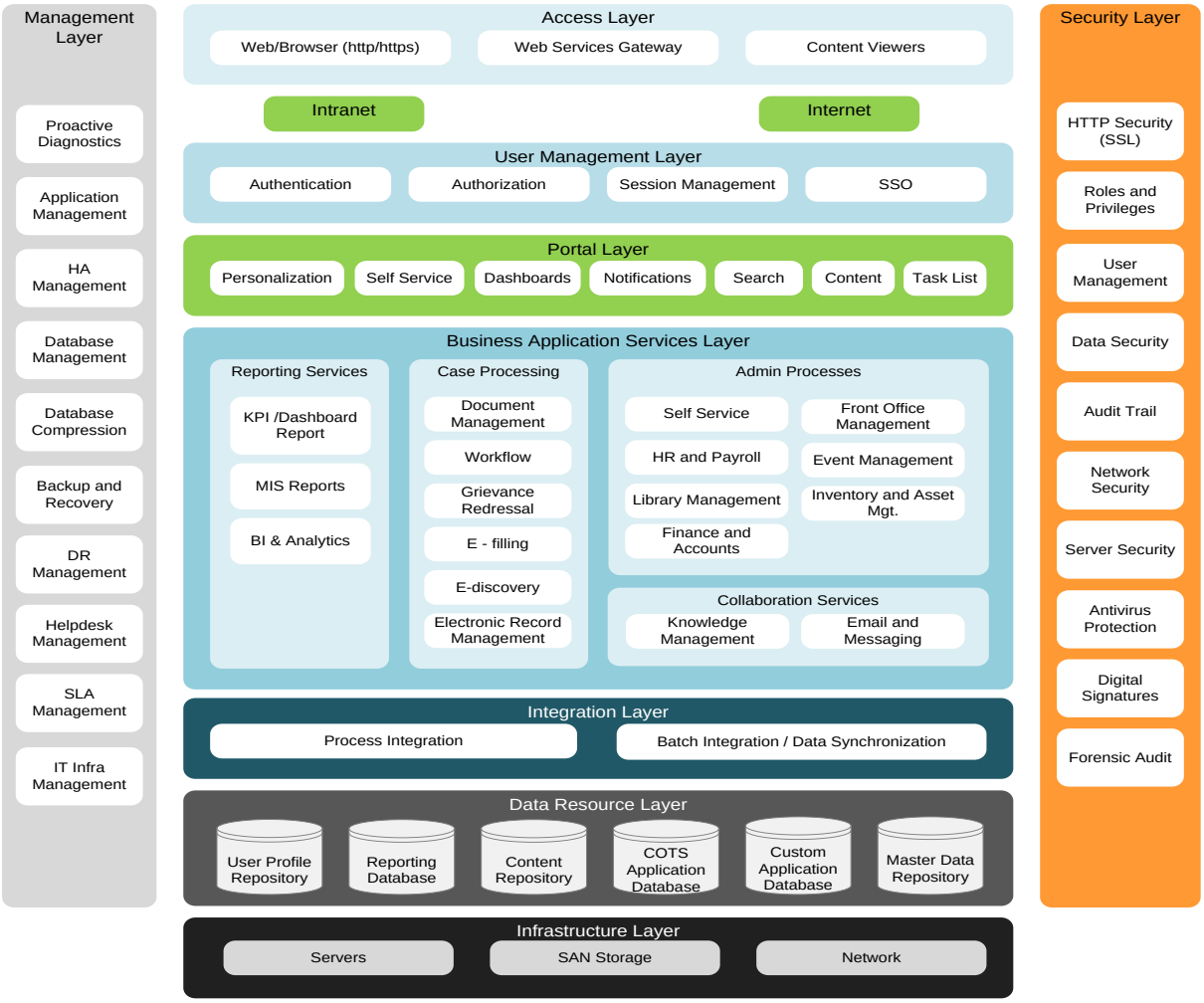
2.1 Application Architecture

i. One of the technological challenges in implementation of e-Governance is to manage the large number of applications that need interoperability to interact with each other while maintaining security and privacy of the data. This needs to be accomplished in such a manner that change requirement in a single application should not trigger changes in other applications. The Service Oriented Architecture (SOA) architecture fulfils this requirement.

ii. The specifications for Hardware, Software and Network components are given in detail in the Volume 2 of this report.

iii. The provisions of Security would be as per the guidelines of Government of India.

Thus all the applications should comply with the SOA. The indicative application architecture is given in the figure below:



The proposed solution comprising application software should be process oriented and based on workflow management. The workflow system should be able to handle routing

of documents, structured information handling, complex event processing, programmatic manipulation of information, and the ability to exchange information with web services and other external information sources.

The entire portfolio of applications specified here in should be able to provide procedural automation of all the existing business processes i.e. work flow activities, invocation of appropriate human and/or IT resources associated with the various steps in an activity. The proposed solution should be able to easily respond to changes of user's need.

The document has been divided in different modules for purpose of specifying different kind of business activities for ease of understanding but each of the modules is a part of one integrated solution. The workflow system should be able to interact between different processes and data base to carry out required task.

The scope of integration includes establishment of Business Services following SOA principles. Service oriented architecture would be preferred solution for work flow implementation. SOA with its loosely coupled nature shall provide better flexibility in building applications and allow enterprise to plug in new services or upgrade existing services in a granular fashion to address the new and changing business requirements, shall bring better reusability of existing assets or investments and allow to create applications that can be built on top of new and existing applications without completely rewriting an application.

Service Oriented Architecture shall be implemented using standard set of technical specifications of Web Services to achieve a platform neutral approach for accessing services and better interoperability. SOA should be approached based on business process as the driver and it should not be driven purely from an IT perspective (i.e., reuse only.

Applications, systems and infrastructure are to be characterized as service-oriented, component based & reusable. The system will be modular in design, operations and implementation.

Also the variables in business rules embedded in these services should be configurable and not hard-coded.

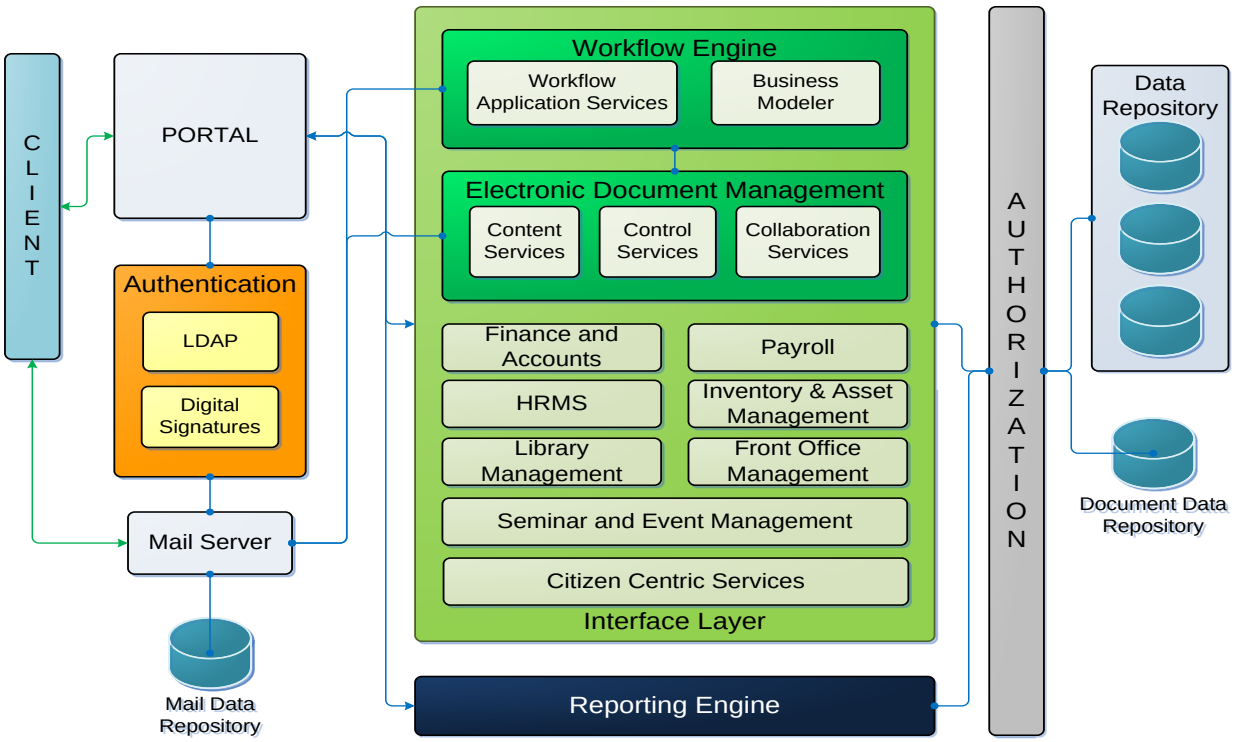
2.2 Functional Architecture

There should be following elements in the Functional Architecture:

a. **Citizen Interfaces:** It is expected that the citizen centric services would be accessed by the citizen through various channels. The Citizens should also be able to access the services directly by accessing the web portal or through mobile devices.
b. **Department Interfaces:** The division at the backend need to access the system for various purposes like data entry, data updation, case processing, approvals through workflow etc. These interfaces can be via the Internet or through an Intranet.

c. **Basic functional elements:** The service delivery demands 24x7 availability of the system, authentication and authorization of various classes of users, workflow system for approvals, digital signature/PKI for authenticating records/ certificates, payments to be made, MIS, Dashboards for monitoring and mobile services.

Functional Solution will be portal based. The authenticated users will access the applications via portal based on the defined roles. Authorization layer will validate that only the authorized data is accessed by the users. The indicative high level illustrative representation of Functional Architecture is in the figure below:



2.3 Deployment Architecture

The deployment architecture envisages leveraging of the core components of NIC Data Centre. The applications and their data under this project shall be hosted at the NIC and both the offices shall be connected through the MPLS-VPN network.

The servers required for hosting the applications at NIC DC are indicated below. The quantity is indicative and minimum configuration is listed in Hardware Specifications. Based on the solution design of the System Integrator these may change.

Server	Applications	Fail Over	Count
DMS, Workflow and Portal Server	Document Management System, Workflow, Portal	Yes	2
Database Server	Database Enterprise Edition	Yes	2
Other	HRMS, Payroll, F & A, Lib. Mgt.,	Yes	2

Application Server	Front Office Mgt., Inventory and Asset Mgt., Seminar and Event Mgt.		
Messaging Server	Messaging Application	No	1
Data Leak Prevention Server	DLP Solution	No	1
LDAP & DNS Server	LDAP	Yes	1
Forensic Analysis Server	Forensic Analysis Software	No	1
Analytics Server	BI and BA	No	1
VPN Appliance			1

It is suggested that the IT components at DRC should be exact replica of the DC facilities with NIC. The RTO and RPO would be the same as per NIC policies applicable to disaster recovery procedures.

The following servers required for hosting at CCI Office are indicated below. The quantity is indicative and minimum configuration is listed in Hardware Specifications. Based on the solution design of the System Integrator these may change.

Server	Applications	Fail Over	Count
LDAP Server	LDAP	Yes	1
Antivirus Server	Antivirus Application	No	1
DMS Cache Server		No	1

The LAN setup should be built to provide Non-blocking architecture and should be Modular & scalable. The LAN should support IPv6 and provide 100/1000 mbps connectivity to end users. The LAN Setup should be designed with Core, Distribution & Access layers with component level redundancy as shown in the diagram below. Also considering the user loads the core and distribution layers may be merged and if the user load increases this can be scaled up by separating the distribution layer from the core layer and adding required number of switches in the distribution layer.

The network requirements for Upgradation of existing LAN are indicated below. The quantity is indicative and minimum configuration is listed in Hardware Specifications. Based on the solution design of the System Integrator these may change.

Equipment	Quantity
Internet Router	2
Core Switches	2
8 Port Giga Ethernet Switch	2
Central Router for MPLS – VPN	2
Wireless Access Points	18
Wireless LAN Controller	1

An UTM with IPS and Firewall at the gateway would provide the necessary security for the servers.

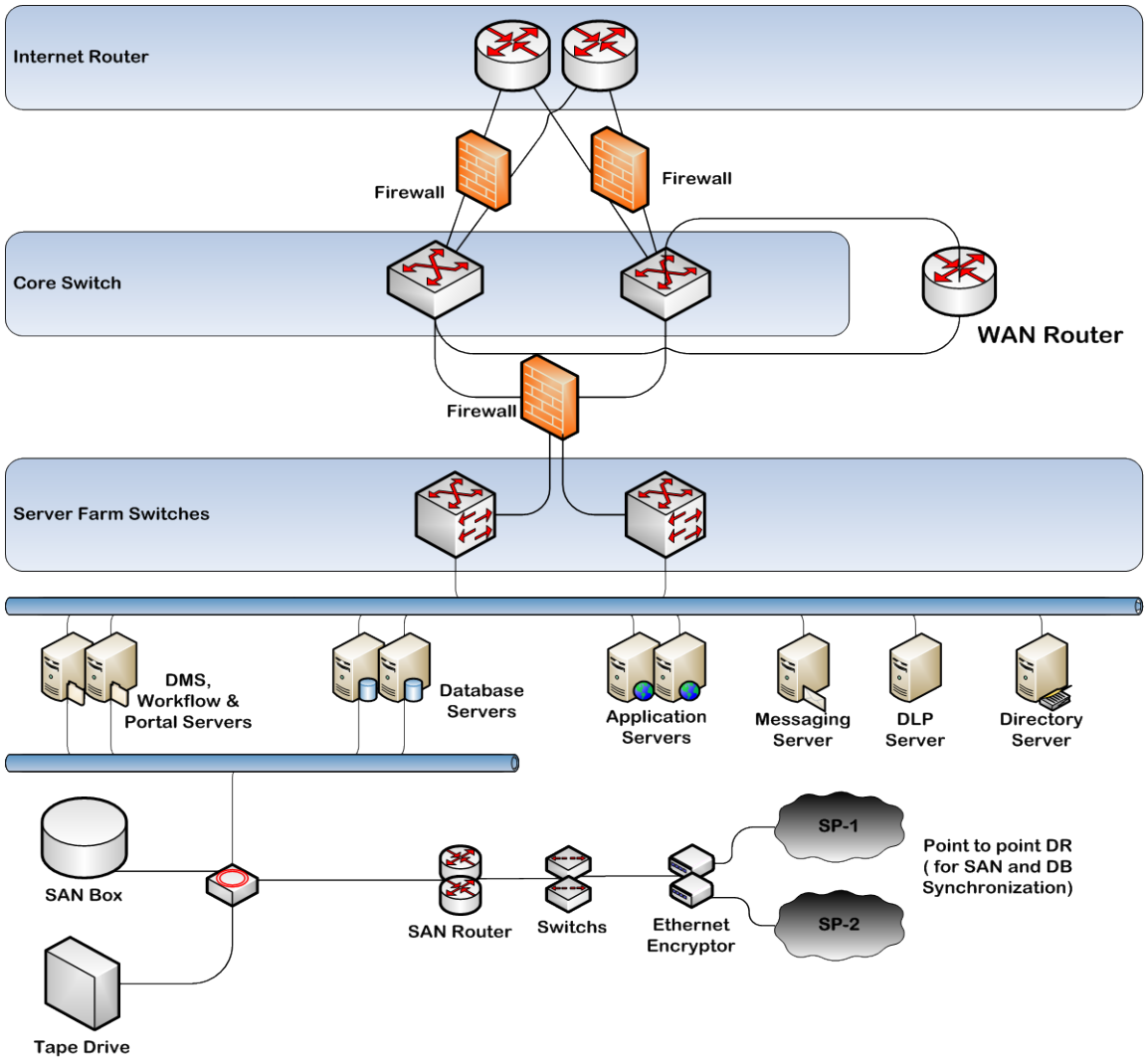
The identified Bandwidth requirements are indicated below, the SI has to recommend based on the solution proposed:

- Bandwidth of 8 mbps MPLS is recommended between DC and CCI Office
- Bandwidth of 8 mbps MPLS is recommended between CCI Office and DG Office
- Internet Bandwidth of 10 mbps is recommended at CCI Office which will be shared with DG Office via MPLS link

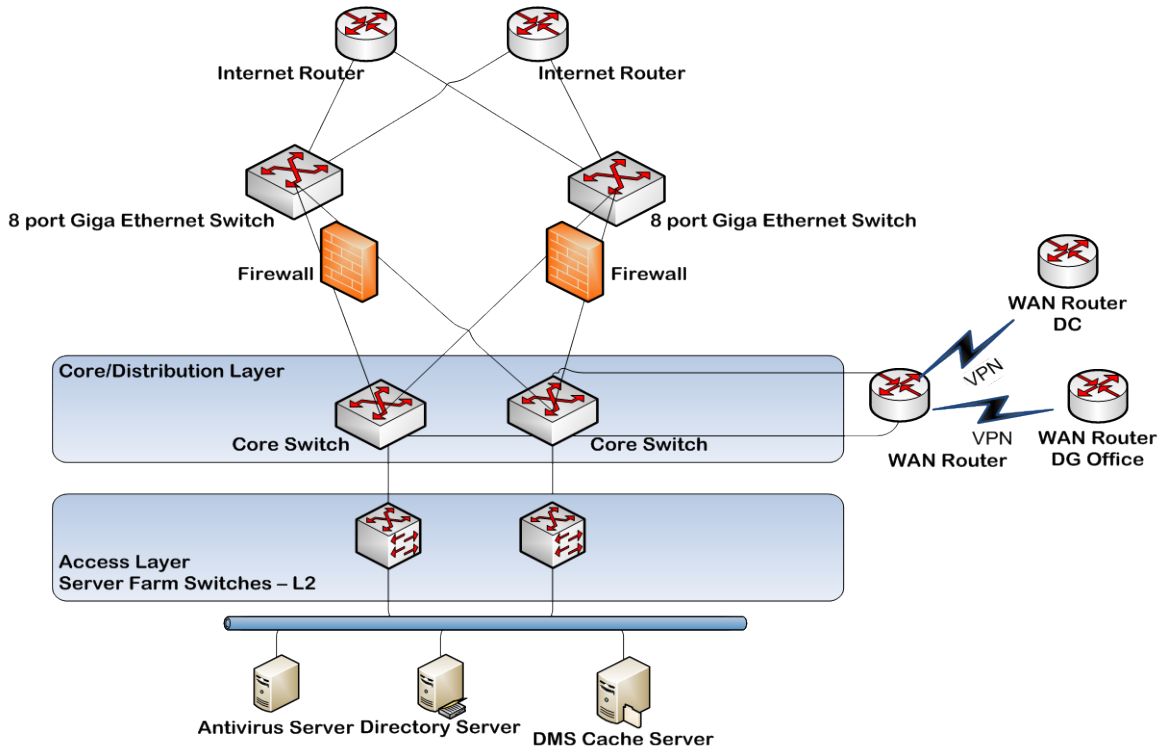
The printers and scanners will be sharable in a setup of print servers and scan servers, and centralized network print and scan management tasks. Print and Scan Server (part of LDAP Server) will enable you to share printers and scanners on a network. Atleast one network enabled multifunctional printer should be deployed per division and should be connected with the Print and Scan Server (LDAP Server). The existing multifunctional printers/scanners should also be connected to the server.

The indicative network architecture of Data Centre and CCI Office is shown in the figures below, the Supplier has to propose the best possible architecture based on his solution design:

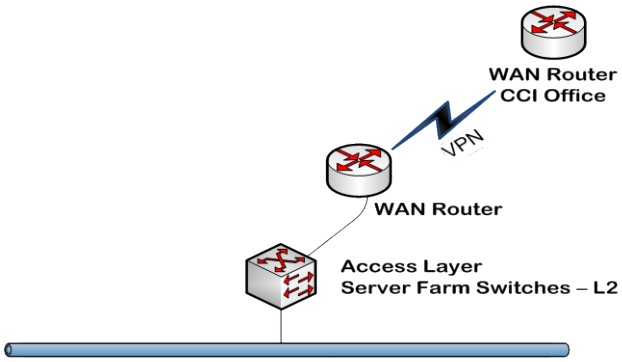
2.3.1 Data Centre



2.3.2 CCI Office



2.3.3 DG Office



3. General Specifications

S. No.	Features	Compliance Code
1.	The solution offered shall be uni-code compliant	
2.	The solution offered should be Service Oriented Architecture compliant	
3.	The solution shall support N-tier and Internet architecture	
4.	The solution should support application and database clustering and load balancing	
5.	The Solution shall provide an application architecture which 'can' be integrated with third party / using the built-in middleware technology	
6.	Workflow including approval with thresholds shall be an integral part of the solution and shall interface with email systems supporting SMTP and IMAP	
7.	The Solution should include tools / mechanism for System, Database and performance measurement activities	
8.	Ability to maintain audit-trail of all transactions and activities	
9.	Ability to generate report output directly in excel, PDF, text, Work sheet, XML ,HTML or such other file types	
10.	The system must have a user friendly web based access.	
11.	The future versions of the solution shall support functionalities provided in the earlier versions	
12.	Ability of the solution to work concurrently with any other software for functioning e.g. Anti Virus, Firewall MS-Office	
13.	Ability of the solution to provide XML based web-services which can be used by other applications	
14.	Must be able to extend capability to support secure (encrypted) access to the portal over the Internet/Intranet through a secure remote access on-demand access to applications (Web and TCP/IP) without the need to add any client software on the desktops.	
15.	Should provide a complete set of integration services, including integration with Web Services, HTML & XML sources, and syndicated content – without modifying the underlying applications.	
16.	Should provide single sign on to system through portal	
17.	The system should be scalable to allow increase in the number of users to at least 3 times current number of users.	
18.	The system should be scalable to allow an increase in the volume and data load to at least 3 times of the volume and data load in the first year.	
19.	The system should be based on open standards to provide interoperability with multiple platforms and to avoid any technology or technology provider lock-in.	

20.	The system should comply with industry standards prevailing at that time unless not technically feasible. Certain indicative standards that are not intended to be exhaustive are listed below: • Security – ISO:27000 • International records management standard - ISO15489-1 • Generally Accepted Recordkeeping Principles (GARP): Framework for managing records in a way that supports an organization's immediate and future regulatory, legal, risk mitigation, environmental and operational requirements. • WfMC Interoperability of workflow management systems • BPEL Standards • ITIL - IT Service Management • COBIT 5 - IT Governance and Control • ISO 19005-2:2011 - Use of the Portable Document Format (PDF) • World Wide Web Consortium (W3C) and GoI Standards for Website and Portal • Content Management Interoperability Services (CMIS) • Project Documentation – IEEE/ISO • ISO 9000 for Quality Assurance • AES, PKCS standards for document encryption	

4. Software Specifications

4.1 Document Management System and Workflow

CCI's business involves dealing with voluminous documents and generation of plethora of documents content and other paper-based information which needs to be classified, synthesized and managed.

Document management solution is required to store and access electronic documents and/or images of paper documents; provide storage, versioning, metadata, security, as well as indexing and retrieval capabilities.

Document management systems comprising tools, technologies and applications will be used to capture, store, manage, preserve and deliver content to user segments. The electronic documents created and generated will be used for various purposes. The broad system functionalities and essential features required to meet CCI needs are given below:

i. Capture: scanning/upload of content, eForms submission
ii. Storage: adequate storage space so that users can add documents as per their requirement.
iii. Easy Additions: Adding a new Document should be easy and trouble free so that user can upload the document file at ease.
iv. Managed Filing: Document filing system can be maintained hierarchy like normal disk based file systems and also associate documents
v. Fast Retrieval: User should be able to search for any document that has been uploaded by name with Full Text Search of inside any kind of document. Automated Retrieval should also available by popular XML formats like RSS for every Tag.
vi. Security: Each document must be protected by a granular security system,-all Documents must be protected against theft, loss and tampering.
vii. Distribution: The documents must be available in internal and external portal, depending upon corporate policy, to any user who has access right to it. It should also be possible easily click-to-distribute documents to select users, user group.
viii. Version Management: Automatic Revision control system must be in place that maintains versions automatically, every time a document is updated. All prior revisions should also be always available
ix. Retention: The facility of purging prior revisions and permanently deleting stored documents should also be available to user to protect security of sensitive documents.
x. File Collaboration: It should be possible to collaborate on any kind of document that is stored within using ad-hoc Workflows of Collaboration.
xi. Workflow and Electronic File Movement: movement of content in defined business process

Workflow Management System should also work independently and should be able to integrate with other systems like document management systems, databases, e-mail, etc.

WMS should have a Visual business process editor to help define, manage, control and coordinate different activities associated with various business processes. The execution

of activities in the process flow are pre-defined in WMS system and this enables transparency in planning and control of every aspect of an enterprise, especially where users work together and share information.

DMS and Workflow applications should be based on platforms offered by Newgen Technologies and Oracle.

4.1.1 Technical Specifications

S. No.	Functionality	Compliance Code
	System Architecture	
1.	Should have the functionality of the distributed repository (object stores) to manage objects - documents, directories and special facilities.	
2.	Should support integration with systems for data storage and content including WORM etc.	
3.	Should have a central repository for storing all kinds of content and functionality must have access to the repository via a web user interface.	
4.	Should have the functionality of the distributed storage of content in memory to accelerate access.	
5.	Should be flexible and object-oriented data model.	
6.	Should have the functionality of version management for objects that are organized and stored in the content management repository.	
7.	Should have the functionality of managing relationships between related objects that are stored in the repository.	
8.	Should have the functionality of the automatic classification of XML content.	
9.	Must have the functionality of the rendering of various types and formats of content in PDF, HTML and other formats.	
10.	Should have the functionality of a document lifecycle management.	
11.	Should have the functionality to create customized searches through a graphical user interface. Also should support the full-text search by content.	
12.	Should have the functionality to define authorization for access to facilities to the level of object attribute values.	
13.	Should have the functionality of logging of events for the content and processes.	
14.	Should have the functionality of XML-based import and export.	
15.	Should have the functionality for managing business processes that is based on the server architecture.	
16.	Should have the functionality of individual and group work management tasks.	

S. No.	Functionality	Compliance Code
17.	Should have the functionality of BPEL/BPEL4S - consistent with the orchestration process.	
18.	Should have the functionality of inheritance for definition of business processes.	
19.	Should have the functionality of the detection limits for processing tasks, and depending on the deadline, must be able to make exceptions to the process - send notification to the user, run an extra process if required	
20.	Should have the functionality to define the limits and timers for individual tasks, group tasks, and the whole process.	
21.	For analysis of business processes should have the functionality of the collection and organization of statistical data using OLAP cubes.	
22.	Should have the functionality of integration with other information systems by using web services.	
23.	Should have interfaces for integration with the system for managing business rules.	
24.	Should have the functionality of import and export configuration.	
25.	Must have a functional organization of business processes in a subfolder.	
26.	Must be able to monitor business processes in real time and the option of reporting the key Milestones.	
27.	Should have a capability for process simulation.	
28.	Should have the functionality of managing e-forms with PKI	
29.	Should support distribution to multiple servers.	
30.	Must support high availability configuration and disaster recovery configurations.	
31.	Should provide authentication services using directory services by industry standards.	
32.	Must support the localization of the user interface.	
33.	Should support the DITA (Darwin Information Typing The Architecture) XML-based architecture for creating and rendering content.	
	Administration	
34.	Should have a graphical user interface for: • administration user interface • administration of business processes • administration modules for content management	
35.	Should support the generation of reports using 3rd party tools to generate reports that are compatible with the database.	
36.	Must have the functionality to update security policies, while the system is used (real time).	
37.	Should have the functionality of monitoring systems in real time.	
	Security	

S. No.	Functionality	Compliance Code
38.	Must support authentication using industry standards.	
39.	Should support the SSO (Single Sign On).	
40.	Must have the functionality to deny access to documents and folders based on user names or belonging to a group of users.	
41.	Should have the functionality to define the security rights at the document/directory using access control lists for each object.	
42.	Should provide an explicit exclusion of users and / or groups with access to the list of required documents and / or directory.	
43.	Should provide a provision to administrators for retrieving the raw data / documents from database/repository without use of application or any interface.	
44.	Should have the functionality of the control of security policy document with regard to the version of the document.	
45.	Must have the ability to administer users directly in LDAP and not rely on periodic batch import in the system.	
46.	Should have the functionality for user authentication using SSL (Secure Sockets Layer) encryption.	
	Data Storage	
47.	The content should be stored in the original file format	
48.	Should enable access to content without having to be the physical location of content on the site from which you access the content.	
49.	Should enable the storage of content in various formats including text files, spread sheet files, videos, audios, binary and others.	
50.	Must support a variety of systems to store content, including file systems, databases and archive systems.	
	Version Management	
51.	Must support version control - major and minor versions must be supported.	
52.	Must automatically generate the next available version.	
53.	Must provide access to all versions of the document.	
54.	Should support check in / checkout of the version controlled document.	
55.	Should not allow more than one user at the same time to check out the same document.	
56.	Should have functionality that allows "read only" access to the document which is in the check-out.	
	Manage Metadata	
57.	Should have the functionality of storing metadata on documents and directories.	
58.	Should have the functionality to create user metadata.	
59.	Should support multiple types of metadata.	
60.	Should support a class hierarchy that supports inheritance.	
61.	Should support metadata that can have multiple values.	

S. No.	Functionality	Compliance Code
62.	Should support the object metadata, for example, document metadata can be a document or folder.	
63.	Should support the functionality to create your own classes that allow defining the object as an "object".	
64.	Should support the functionality to define a default attribute value	
65.	Should automatically assign a unique global identification number of the document.	
66.	Should have the functionality to monitor content that is not physically stored in the system.	
67.	Should be supported by documents with more content. A document with more content has an identification number but has more than one electronic document.	
	Search	
68.	Should have the functionality of search content including full-text search by content.	
69.	Should support the search of objects according to attribute values and system attributes.	
70.	Should have the functionality to index the multiple versions of a document for the "full text" search.	
71.	Should have the functionality to automatically index the document after check in for purposes of "full text" searches.	
72.	Should have the functionality to crawl the content attribute for the "full text" indexing.	
73.	Should take the form of a search with a predefined criteria, should also have the functionality to search results displayed as a list.	
74.	Applications should have templates for search that allows the user to pre define search criteria.	
75.	Should support Boolean operators AND, OR and NOT to define the search criteria.	
76.	Should limit the search results according to security rights that users have.	
77.	Should support the following search operators: Equal, Not Equal, Greater Than, Less Than, Greater or Equal, Less or Equal, Like, Not Like, Is Null, Null and Is Not.	
78.	Should allow the user to choose which attributes to display the document in the list that displays search results.	
79.	Should have the functionality of a combined "full text" and search by attributes.	
80.	Should support the search for multiple words and phrases.	
81.	Should support the search, which excludes the contents of documents that have the specified word / phrase.	
82.	Should support the search for words that are next to each other.	
83.	Should support the search for words that are in the same sentence / paragraph.	

S. No.	Functionality	Compliance Code
84.	Should support one or more search words in HTML or XML files.	
85.	Should have ability to sort on Search results	
86.	Should have ability to page search results	
87.	Should have ability to customize look and feel of search results without code	
88.	Should have ability to save search results	
89.	Should have ability to directly check out a document from search results	
	Directory Management	
90.	Should have the functionality to organize the multi-level directory under the directory.	
91.	Should have the functionality to ban from the directory belonging to user groups.	
92.	Should have the functionality of the document can be saved in more than one directory.	
93.	Should support the storage of documents in the directory and store directories of the directory.	
	Integration	
94.	Should have an XML Web Services API.	
95.	Web Services API should have the functionality to multiple objects (and their contents) can be downloaded in one operation, and also that multiple updates can be done in one pass.	
96.	Web Services API should have the functionality that each request is independent of each other so that they can distribute load among multiple servers.	
97.	Web Services API should have the functionality of replication on multiple servers so that client requests can be directed to different instances of web services.	
98.	Should have industry standard APIs.	
99.	Should have a (Web Distributed Authoring and Versioning) WebDAV service.	
100.	Should have the functionality to integrate with other corporate systems	
	Business Process management	
101.	Should have the functionality of the design, implementation, simulation, optimization and re-deployment of business processes.	
102.	Should have the functionality of public mailboxes allocation and management of group work tasks.	
103.	Should have the functionality of the private boxes for the award and manage individual work tasks.	
104.	Should be supported to carry out simple (review, approve) the business processes.	

S. No.	Functionality	Compliance Code
105.	The graphical user interface should have the option to interface for analyst's business process (easy) and designers of business processes (with the functionality to implement).	
106.	Should have the functionality to escalation and prioritization of tasks.	
107.	Should have the functionality to automate tasks.	
108.	Should have the functionality of tracking the status of active tasks and files.	
109.	Should have the functionality to store all user actions undertaken in processing tasks (audit trail).	
110.	Should have the functionality to view statistical reports on work assignments.	
111.	Should be able to react to system events such as timers or entering a new document in the system.	
112.	Should have the possibility of conditional branching in business processes.	
113.	Should have a graphical interface for modelling business processes.	
114.	Should have support for modelling and simulation of business processes by using thin clients.	
115.	Should have functionality to reuse the defined process clause or sub-process.	
116.	Should have the functionality to allow end users to design processes without the need for programming.	
117.	Should have the functionality to view the mailbox with working tasks to carry out specific user (Inbox) or groups of users (Queue).	
118.	Should ensure that tasks can be seen only by those users / groups who do have security rights.	
119.	Should have the functionality so users can view all active processes that he started.	
120.	Should allow users to view documents and / or directories that are attached to the process.	
121.	Should allow users to make check in / out documents that were attached to the process.	
122.	Should provide an overview and update fields that are defined for the task.	
123.	Should have the functionality for end-user displays instructions on how to perform a specific task.	
124.	Should have the functionality that the user can see which are the key point to be reached in a particular process.	
125.	Should have the functionality that users can work on assignments from the public to switch to a private compartment tray.	
126.	Should have the functionality for adding and changing participants	

S. No.	Functionality	Compliance Code
	of the process until the process is active.	
127.	Simulator should support the use of real data stored in the database for the analysis process, should also support the simulated data or data that defines the user.	
128.	WEB 2.0 user interfaces should have the functionality of the automatic linking of independent components of the user interface.	
	Document Workflows	
129.	Should have a parallel routing functionality in business processes.	
130.	Should support for simple single step workflows for review and approval.	
131.	Should have ability to associate workflows with different Document Types	
132.	Should have ability to obtain collective review feedback on a document from multiple reviewers.	
133.	Should have ability to trigger a document workflow manually or automatically (for example upon upload or edit).	
134.	Should provide support for recording and displaying Workflow History	
135.	Should provide support for assigning, viewing tasks and alerting users on tasks	
136.	Should provide support for common workflow actions such as sending e-mail notifications, copying, moving documents, conditional branching and looping of actions, and others as per CCI requirement	
137.	Should have functionality to automatically trigger workflows from office clients without any configurations	
138.	Should have support for Work Queues and task prioritisations	
139.	Should have the functionality to hold the events in the process for synchronizing with the activities of the external systems.	
140.	Should support the design and organization processes with sub-processes.	
141.	Should support multiple document attachments in the process.	
142.	Should support multiple attachments folder in the process.	
143.	Should have procedural points that have the functionality for content management.	
144.	Should have poured process that can access and update data in the database.	
145.	Should have support for manual and automated processing point.	
146.	Should have the functionality to route tasks to multiple users and systems simultaneously.	
147.	Should have the functionality for processing tasks to the next step in the business process.	

S. No.	Functionality	Compliance Code
148.	Should have a tool to monitor who and what is done in a particular item of business processes and when the task completed.	
149.	Should have the functionality that allows messages from external systems can run the business process.	
150.	Should have the functionality that enables business process to change at any time without affecting the operation of end users.	
151.	Should have the functionality for systematic version control of processes.	
152.	Should support the ballot (voting) more users to make decisions that affect the routing process.	
153.	Should have the functionality to send e-mail alert users to predefined events: reminders of deadlines, exceptions in the process, reaching a critical point (milestone)	
154.	Should have the built-in support for digital signature at Approval Step.	
	Content Management	
155.	Should have a thin client for end users to access functionality for managing content and business processes.	
156.	Should be able to view multiple portlets with different functionalities that can be customized to meet customer needs.	
157.	Should allow users to select multiple documents and work on them simultaneously.	
158.	Should allow users to perform check in / out.	
159.	Should allow users to declare the record automatically when you add content that you create a check-in.	
160.	Should allow users to cancel the check-out.	
161.	Should have the functionality to display a list of documents that are in check out the status of a specific user.	
162.	Should have the functionality to create links to other objects.	
163.	Should allow users to declare the contents as a record.	
164.	Should allow users to designate specific versions of content as a record.	
165.	Should have the functionality to: delete the content, delete versions, degrading version, download content, store content in a directory, to promote version, published in PDF or HTML format.	
166.	Should have the functionality to record changes in the content without promotion to a higher version - check-in.	
167.	Should have functionality that end users can send documents to system via e-mail.	
168.	Should have functionality that allows users to move documents from one folder to another.	
169.	Should provide a simple graphical user interface that allows users to change the security attributes of the documents or folders.	

S. No.	Functionality	Compliance Code
170.	Should allow end users to check out documents that are copied to the workstation or network drive.	
171.	Should have functionality that will allow users to send e-mail in which the attachment links (link) to the document.	
172.	Should have the functionality to run a business process for the selected document or folder.	
173.	Should have functionality that allows end users to define the screens and options that you see when you add or do check in the document.	
174.	Should allow users to view each version of the document.	
175.	Should allow to display list of documents in a thin client with status indicator that shows if the document is checked-out or not	
176.	Should allow end users to see information about who made the check out the document.	
177.	Should allow end users to update the attributes of any version of the document.	
178.	Should have the functionality to display the reference list with links to facilities (favourites) that users are held for their own purposes.	
179.	Should have a Web Application Toolkit, which has functionality that allows you to customize, reuse existing modules and develop new Web applications.	
180.	Should have integration Application Toolkit with APIs that enable integration with other client applications.	
181.	Should have functionality that administrators can allow users to allow or restrict access to functionality and views with regard to their role.	
182.	Should have a functionality that will list only those documents / folders that the user has adequate security rights.	
183.	Should have the functionality to list all the directories in which there is a specific document.	
184.	Should have the functionality to enable users to check in / out all the documents in a folder in one operation.	
185.	Should have the functionality to enable users to cancel check out all the documents in a folder in one operation.	
186.	Should allow sorting of content by clicking on the column headings.	
	Viewer	
187.	Should have a picture viewer.	
188.	Image Viewer should support annotations, including: highlighting, text, lines, arrows and seal.	
189.	Image Viewer should allow viewing of documents with or without annotation.	
190.	The browser should support the rotating of pictures (Clockwise /	

S. No.	Functionality	Compliance Code
	Anti-Clockwise).	
191.	Browser should support display thumbnails (thumbnail view).	
192.	Your browser should have the functionality that the annotation implements security policies so that only authorized individuals can view, modify or delete.	
193.	Should also have the functionality of Zoom-in or Zoom-out	
194.	Should have the functionality to drag and drop for listing the contents of the directory and move between directories.	
	e-forms	
195.	Tools for designing e-forms should not require programming for the replication of paper forms into online HTML forms.	
196.	Application forms will be templates and data stored separately.	
197.	E-forms should have the functionality so that users can use a graphical interface for processing tasks.	
198.	E-forms should have functionality that allows users to create and search external databases.	
199.	Should support data validation	
200.	e-Form should be HTML based without having to install additional third party applications or plug-ins.	
201.	E-forms should be stored in XML format.	
	Coverage Paper Scanning	
202.	Scanning system should have the functionality of scanning thousands of pages of documents in a day.	
203.	Scanning System must support scanning, indexing and storage of scanned documents in a group (batch) or individually.	
204.	Scanning system should have the functionality of saving scanned images in the repository.	
205.	Scanning System should have functionality that supports scanning, indexing and storing at the same time on multiple workstations.	
206.	Scanning System should have functionality to improve image: black border removal, Deskew, deshade, despeckle, destreak, line removal, character reconstruction, edge enhancement and image filters for character smoothing, thickening, and thinning.	
207.	Scanning System should have functionality that allows verification of image quality control of scanned documents.	
208.	Scanning system should have the functionality to identify and remove blank pages.	
209.	Scanning System should have functionality for creating procedural steps that must be completed before the document is saved in repository.	
210.	Scanning system should have the functionality of barcode recognition for automated indexing of documents.	
211.	Scanning system should have the functionality of reading data	

S. No.	Functionality	Compliance Code
	from scanned images using technologies like OCR (Optical Character Recognition) / ICR (Intelligent Character Reader).	
212.	Scanning System should have functionality that allows indexing to be done on multiple workstations.	
213.	Scanning system should support the patch code recognition for the separation documents.	

4.2 RFID Tracking Application

The RFID Tracking Application will be used for following:

i. Physical File Tracking
ii. Library
iii. Assets Tracking

CCI needs the ability to track physical files, books, documents and assets etc. using RFID technology.

File Tracking Records Management software should keep track of where all files/items are located at all times and should allow real-time tracking of files as they move around a facility(s) and for files/Item to be easily tracked or found if missing/misplaced.

RFID (Radio Frequency Identification) will be used for identifying unique file folder records/Item. The File Tracking Software should keep track of all files/items based on the location of the reader, and the item being read, as well as the date and time that 'reads' occur. All RFID 'reads' should be updated to the File Tracking Software database.

4.2.1 Technical Specifications

S. No.	Functionality	Compliance Code
1.	Provide a tracking feature to monitor and record information about the location and movement of Physical Files, Books and assets.	
2.	Record information about movements including: • unique identifier of the file or record; • current location as well as a user-defined number of previous locations (locations should be user-defined); • date item sent/moved from location; • date item received at location (for transfers); and • user responsible for the move (where appropriate).	
3.	Be able to define in the classification scheme files and volumes, and must allow the presence of files in these volumes to be reflected and managed in the same way as electronic records.	
4.	Allow both (physical and electronic records) kinds of records to be managed in an integrated manner by integration with Document	

	Management System and workflow.	
5.	Allow a file that is associated as a hybrid with an electronic aggregation to use the same title and numerical reference code, but with an added indication that it is a hybrid physical file.	
6.	Allow a different records management metadata element set to be configured for physical and electronic files; Physical File records management metadata must include information on the physical location of the file.	
7.	Ensure that retrieval of physical file displays the records management metadata for both electronic and non-electronic records associated with it.	
8.	Include features to control and record access to physical file, including controls based on security category, which are comparable with the features for electronic files.	
9.	Support tracking of physical files by the provision of request, check-out and check-in facilities that reflect the current location of the item concerned.	
10.	Support the creation and recognition of RFID codes for non-electronic objects (for example, documents, files and other containers), or should support other tracking systems to automate the data entry for tracking the movement of such non-electronic records.	
11.	Ensure that a non-electronic record is allocated the same security category as an associated electronic record within a hybrid records aggregation.	
12.	Ability to generate various tracking reports	

4.3 Portal

CCI's Portal should be an enterprise portal to provide access for services and applications. Portal should be user friendly and provide a consistent look and feel based on the guidelines published by DoIT.

Application should work on both form based authentication security wherein the authentication parameters for the registered users would be stored in the server.

The portal should also support integration with LDAP Server for domain based authentication. Also the portal should integrate with two-factor authentication or multi-factor authentication where ever required based on the access levels defined.

The 'CCI Portal' will have CCI Login Area (for CCI User) and Citizen Centric Area (for information exchange with the Commission). The detailed features of the portal provided under these three areas are given below:

CCI User Area

For authorized users, following features will be available in the login area of the enterprise Portal:

- Personalization
- Dashboard
- Notifications
- Chat
- Libraries
- Bulletin Board
- Issues / Complaints
- Search
- Live File Tracking window
- All Application Access

G2C: Citizen Centric Services

Citizen centric features that should be available are as under:

- E-filing
- Submit information
- View case / request Status
- Hearing Schedules
- RTI, Public Grievances

The Portal should also provide following interactions:

i. Government to Employees (G2E) for employee self-services
ii. Government to Government (G2G) for interactions with Central/State Government, Statutory Bodies
iii. Government to Business (G2B) for Cases (Antitrust / Combination), Advocacy Events

The portal shall also display new training, initiatives, information, announcements, etc. taken up by any division.

4.3.1 Technical Specifications

S. No.	Functionality	Compliance code
	Platforms supported by Portal	
1.	The proposed solution should be compatible on all the operating systems offered by the bidder in the proposed solution including client machines which are most likely window based system.	
	Multiple Authentication Mechanism Support:	
2.	Built – in Integral Support for multiple User Authentication mechanisms wherein User authentication is handled over an encrypted Secure Sockets Layer (SSL) channel between the client Web browser and the Portal Server's authentication subsystem.	
3.	The Authentication Subsystem should provide support to proxy user authentication requests to existing authentication mechanisms, eliminating the need to populate and synchronize multiple authentication repositories.	

S. No.	Functionality	Compliance code
4.	The following authentication methods must be supported OUT OF THE BOX: • LDAP v3 • Login and password • NIS • RADIUS • X509 Digital Certificates	
	Ability to Support Secure Remote Access On Demand:	
5.	Must be able to extend capability to support secure (encrypted) access to the portal over the Internet/Intranet through a secure remote access on-demand access to applications (Web and TCP/IP) without the need to add any client software on the desktops.	
6.	Should support a “Zero Client Footprint” wherein any application can be accessed by any device (via a Web Browser) without the installation of proprietary client side software.	
	Integrated Encryption Support:	
7.	Should support encryption that uses either the 40-bit or the 128-bit RC5 algorithm (symmetric algorithm).	
8.	The encryption mechanism should support sequence numbers, HMAC message authentication codes, and key exchange and rotation in order to strengthen the security.	
	Integrated Support for Portal Server Administration and Management Capabilities:	
9.	Should provide a Central Web Based Management Console to administer the portal, Identity Management Services and the Directory Services.	
10.	The Web Based Management console must be able to administer the following: • Adding/deleting users • Adding/deleting authentication mechanisms • Policies • Administering logs • Adding new services/applications • Multi-domain definition. • Delegated Administration • LDAP schema mapping	
11.	Should provide support to administer Portal, Identity & Directory services across multiple portals, which can result in saving of time, management and administrative costs.	
12.	Should provide the capability to associate access rules with restricted objects and users, groups, roles, and domains.	
13.	Should provide the capability to delegate Portal Administration to other users, Department Heads or users outside of the organization for hosted portals.	

S. No.	Functionality	Compliance code
14.	Should provide capabilities to enable community creation and management while enforcing policy and access control through a single management console.	
15.	Should provide policy and administration services across the portal with support to /for LDAP v3	
16.	Should enable cross-domain Web Based Single Sign On for Web Based Aggregated applications on the Portal.	
17.	Should provide Role Based Access Control.	
18.	Should be able to create, manage and delegate identities, policies and services and define & assign roles.	
19.	Should provide a single repository for storing and managing identity, policy and service information supporting LDAP v3	
20.	Should provide policy based content and access control	
21.	Should have integrated identity management that enables central user management, while enforcing policy, access control and providing single sign-on.	
22.	Must have both vertical administration and horizontal administration	
23.	Must have Administration Portlets for creating, updating, and managing the index.	
24.	Support for Virtual Portlets	
25.	Should support Portlet caching	
	Development and Deployment Features:	
26.	Should have integral point and click wizards to aggregate the following types of content: • XML • HTML • RSS (Rich Site Summary) • WSDL • Java Server Pages (JSP) • Java Servlet Serviced Components	
27.	Should provide Java APIs or .Net to extend and access various portal services such as logging, authentication and presentation.	
28.	Should provide a standard deployment utility that enables developers to deploy a customized channel or portlet in a standard way to any portal server.	
29.	Should support dynamic deployment of Portlets, wherein new Portlets are instantly available to the end users without the need to reboot the server.	
30.	Must support the Java 2, Enterprise Edition (J2EE) platform	
31.	Must support JSR 168 Portlets framework specifications	
32.	Portlet must have several modes of display, which can be invoked by icons on the portlet title bar: view, help, edit and configure.	
	Integration Capabilities:	

S. No.	Functionality	Compliance code
33.	Should provide a complete set of integration services, including integration with Web Services, HTML & XML sources, and syndicated content – without modifying the underlying applications.	
34.	Should support the integration of existing applications through standard APIs with the Portal Server	
35.	Should have the ability to deliver integrated content, applications, and services through customizable channels or Portlets.	
36.	Must integrate out of the box with the proposed Server for the Messaging Solution.	
37.	Must have the capability to integrate with the proposed Messaging Server via a customized channel or portlet.	
38.	Should provide ability to extend capability to support delivery of content into mobile devices	
39.	Should support URL rewriting for protection of URLs when the internal applications are accessed from the internet web.	
40.	Should provide support for content from other sources to be published as a part of portal	
41.	Should provide WSRP (Web Services Remote Portlet)	
42.	Should support Inter-portlet communication	
	Personalization Features:	
43.	Must enable rule based portal personalization and customization	
44.	The portal solution should have easy to use interfaces for personalization, setting up templates and adding/maintaining users.	
45.	Should provide administrators the ability to "lockdown" channels/portlets for users so they cannot be deselected	
46.	Should provide administrators the ability to pre-configure default views based on the user's role, group, or domain.	
47.	Should provide Campaign management function	
48.	Should provide filtering, rules and recommendation engines that match user to the right content	
49.	Ability to pre-personalize portal according to the user's role and also allow personalization of features and colour/theme preferences links to web sites through menu options etc.	
50.	Rules-based entitlements will control content by dynamically applying access policies based on the user's role or other attributes, the user can also: - • Go to a single place for all content. • Preferences for a user will determine how the Portal looks and feels • Arrange the content and applications to make better sense of the information	
	Search Capabilities:	

S. No.	Functionality	Compliance code
51.	Should provide a secure search engine that enables users to search for content and receive only those results that they are authorized to access (depending on their profile in the Directory).	
52.	The Portal search engine should be Web services enabled.	
53.	The built-in search engine should be able to search the portal's document repository, Portal Content Organizer as well as Website/Intranet content.	
54.	A User should be able to find relevant information from multiple sources with a single search, do parallel searches across data sources, and combine search results into consolidated lists of matching documents	
55.	Portal's indexer must support multi-word indexing for disambiguation and high precision.	
56.	Portal search service must search local documents and Intranet Content as well as Internet content	

4.4 Website

Website provides a public view of the information which CCI wants to share in the public domain with the general public. The existing website should be upgraded to comply with the guidelines published by Government of India and a more secure technology platform. Given below is the checklist of mandatory guidelines outlined by GoI:

S. No.	Guideline
1.	Association to Government is demonstrated by the use of Emblem/ Logo, prominently displayed on the homepage of the website
2.	Ownership information is displayed on the homepage and on all important entry pages of the website.
3.	Complete and self-explanatory title of the homepage (appearing on the top bar of the browser) is provided.
4.	Website is registered under 'gov.in' or 'nic.in' domain.
5.	Website provides a prominent link to the 'National Portal' from the Home Page and Pages belonging to National Portal load in new browser window.
6.	Website has a Copyright Policy, prominently displayed on the homepage.
7.	Due permissions have been obtained for publishing any content protected by copyright.
8.	Source of all documents, whether reproduced in part or full, is mentioned.
9.	Website has a comprehensive Hyper Linking Policy.
10.	The mechanism is in place to check the accuracy of Hyperlinked Content
11.	Mechanism is in place to ensure that there are no 'broken links' (internal as well as external) or 'Page not found' errors.
12.	Website has a comprehensive Terms & Conditions statement, linked from all important pages.
13.	Terms & Conditions statement disclaims responsibility of the content sourced/

S. No.	Guideline
	linked from a non-Government website and clearly indicates whether information available on the site can be used for legal purposes or not.
14.	Website has a Privacy Policy linked from all the relevant pages.
15.	All electronic commerce transactions are handled through secure means.
16.	All information about the department, useful for the citizen and other stakeholders, is present in the 'About Us' section and mechanism is in place to keep the information up to date.
17.	Self-explanatory title of the service is published.
18.	The website provides a complete description of the service along with the procedure to apply for/avail the same.
19.	The website provides the complete title of the form along with the purpose it is used for.
20.	Language of the Form (other than English) is mentioned clearly.
21.	The complete title of the Act (as written in the official notification) is mentioned.
22.	The complete title of the Document is mentioned on the website.
23.	The language of the Document (other than English) is mentioned clearly.
24.	Validity of the Document has been mentioned.
25.	The official title of the Circular/ Notifications is mentioned.
26.	Validity of the Circular/ Notification is mentioned.
27.	Mechanism is in place to ensure that all Tender/ Recruitment Notices issued by the Department are published on the website.
28.	Website provides a complete description of the Tender/ Recruitment notice along with the procedure to apply for the same.
29.	Mechanism is in place to ensure that information on old/irrelevant Tender/ Recruitment notices is removed or moved into the archive section.
30.	News / Press releases are displayed along with the date and these are organized as per the archival policy of the website.
31.	Website has a 'Contact Us' page, linked from the Home Page and all relevant places in the website.
32.	The complete contact details of important functionaries in the Department are given in the 'Contact Us' section.
33.	Mechanism is in place to ensure that all the Citizen Services, Forms, Documents, etc. are registered with the respective repositories of the National Portal.
34.	Mechanism is in place to ensure that all outdated announcements are removed from the website or moved to archive.
35.	All Discussion Forums on the website are moderated.
36.	For every related link, the complete URL of the Home Page/concerned webpage is provided.
37.	Feedback is collected through online forms and mechanism is in place to ensure timely response to feedback/queries received through the website.
38.	The website has a readily available Help section.
39.	Complete information including title, size (playing time for audio/ video), format, usage instructions and plug-in to view the file is provided for

S. No.	Guideline
	downloadable material including documents.
40.	Mechanism is in place to ensure that all downloadable material is free from virus.
41.	Minimum content as prescribed in the guidelines is present on the homepage.
42.	Subsequent pages of the website have the minimum content as prescribed in the guidelines.
43.	Website is free from offensive/discriminatory language
44.	Content is compiled and packaged with citizen orientation.
45.	The Department has a Content Contribution, Moderation and Approval Policy (CMAP) for the website.
46.	Home page and every important entry page of website display the last updated /reviewed date.
47.	Department has a Content Review Policy (CRP) for the website.
48.	All Documents/Reports have a time stamp at least on the main page.
49.	The Departments have a clearly laid out Content Archival Policy (CAP) for the website.
50.	Clear and simple language has been used throughout the website.
51.	The language is free from spelling and grammatical errors
52.	Whenever there is a change in the language of a web page it has been clearly indicated.
53.	Consistency in nomenclature is maintained across the website.
54.	All information, which is of direct importance to the citizen, is accessible from the Homepage.
55.	Information structure and relationship is preserved in all presentation styles.
56.	The meaningful reading sequence is preserved in all presentation styles.
57.	The website should be bi-lingual (English and Hindi)
58.	Documents / pages are in multiple languages and updated simultaneously.
59.	Visual/textual identity elements highlighting the Government's ownership of the website are prominently placed on the page.
60.	A consistent page layout has been maintained throughout the website.
61.	National identity symbols like Flag, National Emblem etc., are in a proper ratio and colour.
62.	Hindi language fonts have been tested on popular browsers for any inconsistency (loss of layout).
63.	Web pages allow resizing of text without the use of assistive technology.
64.	Text is readable both in electronic and print format and the page prints correctly on an A4 size paper.
65.	There is adequate contrast between text and background colour.
66.	All information conveyed with colour is also available without colour.
67.	Alternate text is provided for non-text elements (e.g. images).
68.	Websites provide textual description of audio/video clips & multimedia presentation.
69.	Captions have been provided for all important audio content.
70.	Web pages do not contain any content that flashes for more than three times

S. No.	Guideline
	in a second.
71.	There is a mechanism for user to control scrolling, blinking content.
72.	There is a mechanism for user to control (stop, pause...) audio that starts automatically.
73.	All pages on the website have a link to the home page.
74.	The positioning and terminology used for navigation items and navigation scheme is consistent across the website.
75.	There are no links to 'under construction' pages.
76.	Each page is a standalone entity in terms of ownership, navigation and context of content.
77.	Web pages allow the user to bypass repeated blocks of content
78.	Website has either a "search" box or a link to a "search" page from every page of the website.
79.	Website has an up to date Site Map that is linked to the Home page as well as to all important entry pages of the website.
80.	If the site uses frames, each frame is properly titled.
81.	Website uses Cascading Style Sheets to control layouts/styles.
82.	Website is readable even when style sheets are switched off or not loaded.
83.	Web pages are usable even when scripts, applets etc. are turned off.
84.	Documents are provided either in html or other accessible formats. Instructions / Download details for viewing these formats are provided
85.	In content implemented using mark-up languages the elements have been use according to specification.
86.	Labels have been provided when content requires input from the users.
87.	Time limit for time dependent web functions can be adjusted by the user (also refer exceptions).
88.	Instructions for operating/understanding content do not rely solely on characteristics like shape size location etc.
89.	All input errors are flashed in text.
90.	Functionality of content is operable through keyboard.
91.	Focus is not trapped in any component while navigating through keyboard only.
92.	Purpose of each link is clear to the user.
93.	When any component receives focus it does not initiate change in context.
94.	Changing the setting of a component does not change the context unless the user has been informed of the same.
95.	Metadata for page like title, keywords, description and language is appropriately included.
96.	Data tables have been provided with necessary tags/mark-up.
97.	All components receive focus in an order that preserves the meaning/ operation.
98.	Role of all interface components can be programmatically determined.
99.	The website has been tested on multiple browsers.
100.	Website has cleared Security Audit by certified agency and has a Security Policy. Applications configured to send mail are enabled over SMTP - auth.

S. No.	Guideline
101.	Websites are accessible to the intended audience in an efficient and secure manner on 24x7 bases.
102.	The Hosting Service Provider possesses state-of-the art multi-tier security infrastructure as well as devices such as firewall and intrusion prevention systems.
103.	The Hosting Service Provider has redundant server infrastructure for high availability.
104.	The Hosting Service Provider performs regular backup of the website.
105.	The Hosting Service Provider has a Disaster Recovery (DR) Centre in a geographically distant location and a well-crafted DR plan for the website.
106.	Web Hosting Service Provider provides Helpdesk & technical support on 24x7x365 basis.
107.	All possible security measures have been taken to prevent defacement/ hacking of the website and the department has contingency plan in place for situations like these.
108.	Website ranks in the first five results on major search engines when searched with relevant keywords.
109.	It has been ensured that all stationery of the department as well as advertisements/public messages issued by the CCI prominently display the URL of the web site.
110.	Department has nominated a Web Information Manager as defined in the guidelines.
111.	The website has a website monitoring policy
112.	All policies and plans are approved by Head of Department
113.	The website should have Website Quality Certificate from STQC
114.	The website should be based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India
115.	The website should support HTML5 and compatible with mobile devices

The detailed guideline can be found at the following link:

https://egovstandards.gov.in/sites/default/files/Guidelines/Guidelines%20for%20Indian%20Government%20Websites/GOI_Web_Guidelines.pdf

4.5 Identity & Access Management System and Security System

Protecting business information is critical to CCI. To thoroughly safeguard entire IT environment, there would be need for not just identity and access management capabilities, but also control over how information is used.

The security requirements and standards for CCI are categorized into the following five functional areas:

- Web Access Management - Authentication, Authorization, Web Single Sign-on, Digital Signature.

- User Management Services – password management services, delegated administration.
- Identity Repository – Data repository, directory for storing a subset of user data to support identification, authentication, authorization.
- Workflow Services - Providing the ability to route and approve requests for access by authorized individuals.
- Additional security and technical requirements on data encryption

An authenticated identity will be linked to the services delivered by CCI through the process of "Authorisation".

A "Threat Management" layer will provide real-time protection against identity theft and online fraud. This layer will evaluate the fraud potential of online access attempts and assess the risk based on a broad set of variables. The "Threat Management" layer will perform this task transparently without inconveniencing the legitimate users.

A reference "Application Sensitivity Matrix" for identifying the right level of authentication is provided in Table below:

	Information Sensitivity Level				
	Level 0	Level 1	Level 2	Level 3	Level 4
Who?	Citizens	Informants / Applicants	Employee	Application Users	Application Users
What?	Orders, General Information	Status Tracking, Submissions	Personally Identifiable Information	Non Confidential information	Confidential Information
Suggested authentication method	No authentication required	Single Factor	Single factor authentication	Two-factor: username and password, OTP/Digital Signatures	Multi-factor: biometrics, username and password

4.5.1 Technical Specifications

S. No.	Functionality	Compliance code
	Adapter/ connector Support	
1.	The proposed solution should be compatible on all the operating systems offered by the bidder in the proposed solution including client machines.	
2.	Identity management for user provisioning should have out of the box workflow for automating approvals for user access management, self-registration and self-care functionality for reducing the administrative load and manual intervention.	

S. No.	Functionality	Compliance code
3.	The solution should provide an IDE to design the workflows.	
4.	The proposed solution should support "Workflow Management Consortium (WfMC) TC-1003 Workflow Reference Model standard for workflow implementation".	
5.	Identity Management Solution should have Connector availability for all target systems that need to be managed.	
6.	The proposed solution should provide resource kit or an SDK to add new Resource adapters.	
7.	Identity Management solution should be agent-less architecture and use gateways where agent is required.	
8.	The Proposed solution should be certified as “Liberty Interoperable” and Should be interoperable with other products / solution based on Security Assertion Markup Language (SAML 3.0) for the following profiles: 1. Identity Provider, 2. Identity Provider Extended 3. Service Provider 4. Service Provider Complete 5. Service Provider Extended 6. Enhanced Client or Proxy 7. Attribute Authority Requester 8. Attribute Authority Responder 9. Authorization Decision Authority Requester 10. Authorization Decision Authority Responder 11. Authentication Authority Requester 12. Authentication Authority Responder 13. POST Binding 14. GSA Profile	
15.	The solution should leverage an intelligent indexing system to manage user identities and access privileges, leaving account information with the information owner and thus avoiding the time- consuming effort of building and maintaining another user repository.	
16.	The Proposed solution should provide an automated way to discover and correlate all accounts associated with an individual to speed the account mapping process.	
17.	The solution should use separate repository for user data and audit log information.	
18.	The solution should support open provisioning standard like Service Provisioning Markup Language (SPML).	
19.	The solution should allow enterprise applications and platforms to integrate into the centralized authentication / authorization framework seamlessly. The solution should support both thick client as well as web based applications.	

S. No.	Functionality	Compliance code
20.	The Access Management solution should be capable of running on web servers as well as application servers.	
21.	The proposed solution should provide the ability for pluggable authentication module, and new auth. modules should be able to be added via an SDK.	
	Access Rights Capabilities and Access Control	
22.	The proposed solution must protect sensitive customers' data in accordance with guidelines that will be agreed with the Purchaser.	
23.	On completion of successful logon, the following information should be displayed: • Date and time of previous successful logon. • Details of any unsuccessful logon attempts since the previous successful logon. • Reminder of the user to bring to notice any aberration observed.	
24.	After predefined number of consecutive unsuccessful attempts to logon to a user Id, that user id should be disabled against further use until the same is enabled by System Administrator.	
25.	Terminal / User Id time-out shall occur if a terminal / user ID remains logged onto a system/ application but remains inactive for a predefined time. The screen shall be cleared of any information when time out occurs.	
26.	Software which can be used to modify existing programs on systems / applications, e.g. editors and compilers, shall have access restricted to authorized staff only. Any such software which is not needed for operational reasons shall be removed after the modifications have been made.	
27.	Clear segregation of duties between user groups is necessary to minimize the risk of negligent or deliberate system misuse. In particular segregation must be implemented between: 1. Business use. 2. Computer operations. 3. Network management. 4. System administration. 5. System development & maintenance. 6. Change management. 7. Security administration. 8. Security audit. Where it is operationally not possible to adhere to this policy advice shall be sought from the Purchaser on security. As a minimum, the above segregation shall be enforced at the User Id level i.e. the above functions shall not be allowed from the same User Id.	

S. No.	Functionality	Compliance code
28.	A prescribed warning screen shall be displayed immediately after a user successfully completes the logon sequence to any multi user system, server or database.	
29.	The system shall provide a mechanism to authorize users to access the system, revoke users from accessing the system, and modify the security information associated with users. The system shall also be able to automatically suspend or roll back a reconfigured account that violates policy.	
30.	The system / resources shall provide a mechanism to allow or deny specified user IDs to access the system during specified ranges of time based on time-of-day, day-of- week, and calendar date.	
31.	The system shall provide a mechanism to allow or deny specified user IDs to access the system based on means of access or port of entry.	
32.	For each resource, the system shall provide a mechanism to specify a list of user IDs or groups with their specific access rights to that resource (i.e. an access control list). Solution shall provide for grouping of users and assigning ACL to the group.	
33.	Group ACL should be aggregated to individual user's ACL and in case of conflict, user's ACL shall govern.	
34.	System shall provide both Grant and Deny to a resource.	
35.	The system shall have ability to assign users individual access rights and to define access rights available to users in a role upon their request and approval.	
36.	The system shall have ability for different personnel to view different levels of information based on their job duties.	
37.	The system shall provide a mechanism to modify the contents of a resource's access control list.	
38.	The System shall have ability to associate access-rights definition with a role within the organization and dynamically and automatically change access rights based on changes in user roles. The system shall also have ability to set designated times for changes in access rights or policies.	
39.	System should also use defined rules/ information specific to CCI to determine routing of approvals.	
40.	The system shall be able to compare local administrator changes against a system-of-record of account states to determine if changes comply with approved authorities and policies and shall be able to notify designated personnel of access- rights changes made outside the provisioning solution, if any.	
41.	The solution should provide the capability to do half yearly audits on the lines of ISO/IEC 27001-02 for user accounts.	

S. No.	Functionality	Compliance code
42.	The system shall provide a mechanism to identify all resources in the system that are owned by a specified user ID, the resources to which that user ID is allowed access and the specific access rights for each resource.	
43.	System shall also be able to detect, evaluate and respond to user authority changes made directly to a resource.	
44.	Each resource delivered with the system shall have the most restrictive access rights possible to permit the intended use of that resource.	
45.	The system shall protect all information used for resource access control decisions (e.g., access control lists, groups lists, system date and time)	
46.	The system shall provide policy simulation and 'what-if' modelling of changes, i.e. simulation of effects of policy changes before they are enacted, reporting errors, or potential problems, and ability to resolve before live operations.	
47.	The system shall monitor the following: • Successful logins and login attempts e.g. Wrong user ID / Password, and login patterns • Rejected access attempts because of insufficient authority • All usage by privilege users e.g. powerful access to system utilities or applications • Use of sensitive resources e.g. Access to highly sensitive data • Change to access rights of resources • Changes to the system security configuration • Modification of the package software • Changes to user privileges.	
48.	The system shall have ability to report on roles, rights associated with roles and users associated with roles.	
49.	The system shall have flexible mechanisms to connect to multiple data stores containing accurate information on valid users.	
50.	The system shall have ability to load identity store information on a scheduled bulk basis and to detect and respond to identity store changes in near real time.	
51.	The system shall have ability to retrieve account information from target managed resources on a scheduled basis, both in bulk or in filtered subsets to preserve network bandwidth.	
52.	The system shall have ability to detect and report in near real-time local administrator account maintenance (creation, deletion, changes) made directly on local resources natively.	
53.	The system shall define services that must be granted prior to creation of the access rights. For example, Microsoft Windows rights must be granted prior to granting rights to Exchange Support for entitlement defaults and constraints (each	

S. No.	Functionality	Compliance code
	characteristic of an entitlement may be set to a default value, or its range can be constrained, depending on the capabilities of the entitlement to be granted)	
	User Administration	
54.	A mechanism must exist to allow a range of User Ids to be built with a standard user profiles of multiple categories, e.g. Data entry user, data modify user at the section office, division office etc.	
55.	Where a user Id remains unused for a pre-specified number of consecutive days, it shall be disabled. If no authorized request for reinstatement is received within a further predefined time period, the user Id shall be deleted. The user would be informed before this happens.	
56.	All user Ids shall be set up with privileges that limit the use of the user Id to designated areas only and to ensure that other functions cannot be performed by the user ID for which they are not authorized. Some user IDs have powerful privileges associated with them and these shall only be provided and maintained by the system administrator. To prevent the provision of user IDs with privileges associated to them, when these are not required by the user, any templates used to set up user IDs shall have no default privileges associated with them.	
57.	System shall be able to create unique user IDs using a set of consistent algorithms and defined policies of the owner and not in current use or previous use by the organization and not shared with others. The system shall provide a mechanism to associate specified information (e.g., user name and affiliation) with each user ID.	
58.	Procedures for user account management should define the naming convention for user IDs and the operations practices for provisioning and removing these user Ids.	
59.	User Ids shall not consist of less than a predefined number of characters. The number of characters would be different for normal users and privileged users;	
60.	The system shall have ability to create a single account with multiple authorities governed by different policies.	
61.	The system shall provide a mechanism to administratively disable user IDs and a mechanism for re-enabling or deleting a disabled user ID after a specified period of time. The use of this mechanism shall be privileged.	
62.	The system shall internally maintain the identity of all active users.	
63.	The system shall provide a mechanism to obtain the status of any user ID.	

S. No.	Functionality	Compliance code
64.	The system shall provide a mechanism that allows a collection of user IDs to be referenced together as a group.	
65.	For those systems that have the architecture to support multiple logons per user ID, the system shall provide a mechanism that limits the number of multiple logon sessions for the same user ID. The mechanism shall allow limits for user IDs and groups to be specified. The system default shall limit each user ID to one simultaneous logon session. As per business process requirement, particular machine ID's to permit login by selected users only.	
66.	The system shall provide a mechanism by which the user ID associated with a process can change to a user ID that would provide any additional privileges.	
67.	The system shall be able to assign users to one or more roles and can implicitly define subsets of access to be unavailable to a role.	
	Administration capabilities	
68.	The system shall adhere to open standards.	
69.	The system shall have secure environment for transmitting access changes across the Internet.	
70.	Protection of private user information through secure facilities and sound processes.	
71.	Reports of user rights into external systems, sponsors of users and audit trails of access rights changes.	
	Authentication	
72.	The system shall provide a mechanism to authenticate the claimed identity of a user.	
73.	The system shall perform the entire user authentication procedure even if the user ID that was entered was not valid. Error feedback shall contain no information regarding which part of the authentication information is incorrect	
74.	The system shall provide a mechanism to support the initial entry or modification of authentication information.	
75.	The system shall require a privilege to access any internal storage of authentication data	
76.	System should support two factor and multi-factor authentications (OTP, Biometrics, tokens etc.)	
	Password Management	
77.	System shall be able to securely deliver User Ids and passwords to new users electronically. User Ids and passwords, when conveyed electronically shall only be visible to the person for whom they are intended e.g. after the user has logged on to the appropriate electronic system.	
78.	All electronic information systems and applications shall have a password management system which meets the following	

S. No.	Functionality	Compliance code
	requirements: a) Enforces change of initial password at first logon b) Allows users to select and change their own passwords at any time subsequently. c) Have ability to implement password formation rules to enforce password strength across the organization, e.g. minimum character length of password, password as a combination of numeric, alphabets & special characters d) Have validation routines built in which, as far as possible, check that the password selected is a quality password as defined in a Policy Document to be handed over to the Purchaser at the time of implementation e) Have a confirmation process on changing passwords to cater for typing errors. f) Have ability to deliver password-change success/ failure status to requestor electronically g) Have the ability to enforce password change after every n days. If the password is not changed in the pre specified number of logins then the ID should be disabled requiring re-enabling by System Administrator h) Prevents reuse of passwords within a specified period/ number of times. i) Does not echo passwords to screen or paper. j) Stores passwords in a one-way encrypted form away from the system/ application data files in a protected password file that is access controlled such that no users can read or copy the encrypted contents. k) Prohibit use of null passwords l) Have ability to synchronize passwords for multiple systems to the same value to reduce the number of different passwords to be remembered by the user m) Have a challenge-response system to authenticate a user with a forgotten password by using shared secrets	
79.	The system shall provide no mechanism whereby multiple user IDs explicitly shares a single stored password entry. The system shall provide no means to facilitate the sharing of passwords by multiple users.	
80.	The system shall allow a user to choose a password that is already associated with another user ID. The system shall provide no indication that a password is already associated with another user ID.	
	Directory Services Requirements for Enterprise	
81.	The Directory Server should be LDAP v3 Compliant LDAP server should be able to replicate data between servers and support cascading replication. Should have support for open standards [LDAP v.3, XML]	

S. No.	Functionality	Compliance code
82.	The directory service should provide support for Group policies and software restriction policies. The group policies should have settings to configure various desktop or user related settings via centralized control. These settings will include items like Browser setting, desktop restrictions, program restrictions, admin controls, software deployment etc. It should allow for almost all manual functions to be automated using group policies.	
83.	• Should have support for integrated authentication mechanism across operating system, messaging services. The Directory Server should have out of the box integration with the e-mail server. • Should provide enhanced authentication like Kerberos which support authentication across multiple Operating system like Windows and Unix/Linux. • Should be able to integrate with other Standards based Directory system for synchronizing user accounts and passwords.	
84.	• SNMP support for flexible network monitoring and management. Should support directory services integrated DNS zones for ease of management and administration/replication. • The directory service should support features for health monitoring and verifying replication. • The directory service shall provide support for modifiable and extensible schema	
85.	• Support for Access Control Lists (ACLs). • Support for controlling access to the directory, a sub-tree, entries, attributes by setting permissions for users, groups, roles and location information like IP addresses. • Should provide facility to provide Rights Management Service for documents like Word, Excel etc. on the built on standards like XRML.	
86.	Support for user authentication through user ID/password, X.509v3 public-key certificates, or Anonymous authentication Should support security features, such as support for Kerberos, smart cards, public key infrastructure (PKI), and x.509 certificates	
87.	Should support partitioning into multiple LDAP Repository architectures for scalability. Should support LDAP servers in multi master configuration Ability to keep Replicas in Synch and to enforce Replication updates	
88.	The solution should provide a comprehensive single window Admin tool locally or over internet to administer the directory	

S. No.	Functionality	Compliance code
	services. The Directory services should have APIs to programmatically manage each component of Directory Service. The directory service shall provide support for modifiable and extensible schema both manually and programmatically	
	Audit Trails & Reports	
89.	The system must maintain- • Time-stamped records of every access change request, approval/denial, justification and change to a managed resource • Time-stamped record of every administrative and policy-driven change to access rights	
90.	The system must provide reports on audit trails for users, systems, administrators and time periods, including workflow approvals, rejections, request statistics, policy compliance and Audit reports, User account reports, Access reports and Service reports and also any customized reports based on specific need.	
91.	Audit trail records shall be retained in a tamper proof environment in accordance with the Purchaser's policy for a reasonable amount of time to allow for accountability and evidential purposes. Backup copies shall also be maintained to protect against any accidental or deliberate erasure of data.	
92.	**System Operations**	
93.	Ability to interact with target resources without interfering with their performance.	
94.	Ability to continue to operate without degradation when the managed system is temporarily inaccessible.	
95.	Ability for the managed resources to remain fully functional if the provisioning solution is unavailable	
96.	Responsiveness to users interacting with the provisioning solution features for searches, reporting, approvals, self-service and auditing.	
97.	Ability to load and maintain synchronization with user information from existing human resources and other identity systems, both statically and dynamically.	
98.	Ability to load account and authorization information from existing operational systems, if any, without data entry	
99.	Ability to detect and reconcile accounts created by, and/or changed by, other administrative systems (e.g., the local administration console provided with the managed resource)	
100.	Support for configuration and scalability requirements for large environments and high- availability operations utilizing shared communication capacity on corporate WANs.	
101.	End-to-end security over account changes.	

S. No.	Functionality	Compliance code
102.	Entirely Web-based functionality to allow easy distributed administration on an unlimited scale.	
103.	Integrated functionality that does not require duplicate data entry or manual synchronization of information shared for multiple functions.	
104.	Ability for servers to be inexpensively configured for high-availability operation, including disaster recovery.	
105.	Ability for utilized data stores to be configured for high-availability operation.	
106.	Ability for provisioning solution to maintain accuracy when local administrators maintain privileges to make changes to target resources.	
107.	Resilient communications design between distributed components to withstand network or target resource outages.	
108.	Multi-layered security architecture for operation in a “demilitarized zone” ((DMZ) and for management of users and systems in untrusted environments.	
109.	XML-based extensibility and interaction with external systems	
110.	Use of common and de facto standards for interfaces that are internal and external to the provisioning solution.	
111.	Integration of LDAP directory services as identity stores, access control system authorization stores and internal user account and policy stores.	
112.	Inclusion of a persistent data store or repository for audit trails and system recovery.	
113.	Ability to respond quickly to user interactions including report requests, access change requests, policy changes and password self- service.	
	Audit Trails and Reports	
114.	The system must be capable of generating log trails, which contain details about any read /write access to sensitive data. Details must relate activity to an identifiable person. They must be configurable, so that filters and switches can be used to lower performance overheads and focus on areas of concern. It is important that the audit trail that is generated contain enough information to support after-the- fact investigation of loss or impropriety.	
115.	Where equipment uses a real-time clock to timestamp audit trail and other time related events, the clock should be regularly checked for synchronization with both connected systems and reference clock outside of the system, in this case the Indian Standard time.	
116.	Where the security audit trail becomes unavailable for any reason, the system shall continue to operate but shall trigger an alarm.	

S. No.	Functionality	Compliance code
117.	System and application use and attempted use will be monitored to ensure that the integrity and security of the client and customer data is maintained. The documented process shall include details of: who will monitor what event and how, the frequency of monitoring, what to do when suspicious activity is noted, when to escalate and the escalation path. The log must record the user or process responsible for the event, terminal ID where available, and the date and time of the event. The following shall be monitored :- • Enabling and disabling of the audit process • Any changes to the type of events logged by the audit trail • Any changes to the audit trail itself • Start-up parameters and any changes to them • System or application start- up and shut-down • Use of selected transactions • Changes to any data base or records	
118.	Audit records and journals shall be retained in a tamper proof environment in accordance with the Purchaser's policy to allow for accountability and evidential purposes. Backup copies shall also be maintained to protect against any accidental or deliberate erasure of data.	
	System Integrity	
119.	The system should be able to protect the user process and local data from other user.	
120.	Mechanisms should be in place to ensure that the currently installed software has remained consistent with the delivered product.	
121.	Software used on systems/ applications shall be subject to version and change control to ensure that only the current authorized software is used at all user location.	
122.	Modification or replacement of the software provided with the system would require special privileges	
123.	Execution of system maintenance and repair software would require special privileges	
124.	The system should be able to track the date and time at which a resource was last modified.	
125.	The system should have in-built mechanisms e.g. checksums to verify the integrity of data passed over a communication channel.	
126.	Where an encryption process used for data transfer fails and cannot be automatically corrected, then the transfer should not be completed.	
	Confidentiality	
127.	The system should have the flexibility of encrypting the data stored online.	

S. No.	Functionality	Compliance code
128.	Any cryptographic techniques or encryption systems used to safeguard information shall have been approved by relevant authority on data security prior to their use.	
129.	Only security components which have been approved by the Purchaser shall be used to protect the Purchaser's sensitive information and processes.	
130.	The procedures used to maintain confidentiality should be documented and access to them restricted.	
	Networking and Data Transfer	
131.	All data transfers must be documented and authorized by the owner of the donor system. They must only be authorized where the receiving system has the capability to protect the data, i.e. it has an acceptable security rating.	
132.	Data which is to be passed between systems shall be labelled to indicate the type and sensitivity of that data. The security policy for a system will state what data may be sent to, or received from, another system and will state the translation, if any, between the labelling of the two systems. Interfaces that have been built -i.e. the data migration systems should have defined access rights. The interfaces should have a fixed enabling procedure - including the frequency with which the migration happens to and from the system, the data flow that would happen and the data items that would be frozen during such a migration.	
	Security of web services	
133.	XML based Web security schemes: As web services have certain limitations with SSL type of security scheme, the web service technology shall be used with different XML-based security schemes. Some of the XML- based securities include the following: • WS-security • XML digital signature • XML encryption • XKMS (XML Key Management specifications) • SAML (Secure Assertion Markup Language) • ebXML Message service The bidder shall ensure content security, message level security and secure message delivery, metadata security policy, trust management and secure public key infrastructure while implementing web services using appropriate web security mechanism, which must be W3C / OASIS compliant.	

4.6 Data Leak/Loss Prevention Solution

CCI wants to setup Data Leakage Prevention (DLP) Solution for monitoring of various IT Systems through which critical data flows, resides, generated or being modified. The solution should cover network egress points (gateways, firewalls), email system, Web Proxy, Applications, Partners network, storage system and all End- Points (Desktops and Laptops). The data to be protected will be decided based on the policy framework and after discussions with various departments CCI. Incident reporting and alert generations through various communication mediums and a proactive solution which can work on the basis of predefined or learned policies to protect the business critical data leakage from these systems.

4.6.1 Data on Move

All data traveling on the network via protocols including (but not limited to) FTP, HTTP, HTTP, SMTP, Instant Messaging, etc. The DLP solution is expected to -

i. Identify and Monitor the content of the data being sent by the users
ii. Restrict users from sending sensitive data to external network
iii. Report any violations to the policy defined within DLP

4.6.2 Data at Rest

Data that is stored on the network storage devices (e.g. Shared drives, storage servers etc.), databases, CMS and fixed end-points is termed as Data at Rest.

The DLP solution is expected to perform following tasks:

i. Identify the sensitivity of the data stored basis the policy defined.
ii. Identify the users who have access to the data
iii. Monitor & report the activities being performed on the data.

4.6.3 Data in Use:

Data that is stored on the desktop/laptops issued to the users is termed as Data at End point. A DLP solution is expected to perform following key tasks:

i. Identify the sensitivity of the data stored basis the policy defined
ii. Restrict the activities a user may perform on the data (e.g. Copying to a USB drive etc.)
iii. Monitor & report the activities being performed by the user

4.6.4 Technical Specifications

S. No.	Functionality	Compliance Code
	System Management	
1.	The Solution should have Centralized Management, a single web based console for System Administration, Policy Management,	

	Workflow and Reporting Engine.	
2.	The solution should integrate with the existing LDAP infrastructure for Authentication and provide Administrative roles based on Directory groups. Should have out-of-the-box integration with Cisco Iron Port, Microsoft AD-RMS, and the proposed solution.	
3.	The solution should have Secure Storage of System Passwords and Data Repository. All incident details should be stored encrypted within DLP DB and FileSystem	
4.	The solution should maintain audit logs that track administrator activity within the DLP suite that can provide details on policy modifications, logins, and other administrative activity. The following details should be logged - • creation, deletion, and updating of DLP users • creation, deletion, and updating of DLP groups • creation, deletion, and updating of DLP user roles • changes to the configuration of DLP Network, including creating, deleting, or modifying the configuration • changes to the configuration of DLP Datacentre, including creating, deleting, or modifying the configuration • all logins to the centralized web console including failed logins • creation, deletion, and updating of DLP policies	
5.	The solution should support both agentless and agent based scanning	
6.	Ability to deploy temporary agents for scanning and support incremental scans to speed up the scanning time	
7.	All communication between the agent and the system should be encrypted	
8.	The solution should provide a very fine grained access control allowing creation of roles with any combination of permissions - e.g. • Can a role be created to have access to system administration functions but not to policy, incident, or employee information? • Can a role have the ability to author policies but not to deploy them live on the network? • Can a role be created that allows users to view incidents but not to modify or remediate them? • Can a role be created that has the ability to see summary reports, trend reports and high-level metrics without the ability to see individual incidents?	
	Content Recognition	
9.	Pre-Built Described Content Definitions (ex: GLBA, PCI, PII, etc.) Keywords, regex, entities, dictionaries with Contextual Criteria, Proximity Criteria, Weighting Criteria, Fingerprinting, Fingerprinting Crawler with definable parameters, Databases Fingerprinting with Ability to select Must Have and May have	

	columns. Detection of Encrypted Files and Password protected files	
10.	Detect based on file content and not file extension. The solution should not modify or add to the actual content in any case unless it requires encryption and/or quarantining.	
11.	Index corporate directory information (LDAP/AD, groups, geographies, etc.) to include/exclude specific employees in a policy	
	Policies	
12.	Out of the box predefined Global Policies like BASEL III, PCI, SOX, PII and Policies related to company financials and confidential data.	
13.	Custom Policy definition upon File type (extension and true file type) , Network Destination - sender/recipient IP and/or email address, Transmission attributes, protocol types, Identity per LDAP user and groups, content type, Risk and Severity	
14.	System should allow for configurable scoring of incident severity based on ALL of the following - - Amount of data records exposed - Specific senders or recipients - Network protocol - Specific records that were exposed - Specific documents that were exposed - Custom LDAP attribute - Network Source and Destination	
15.	The solution should support inclusion and exclusion detection rules based on corporate directory data to enforce policy based on any attribute of senders or receivers such as business unit, department, job level, employment status, security clearance, geography, or employee vs. contractor	
16.	The solution should have predefined detection policies to cover regulations and detection best practices, including pre-defined lexicons for commonly required regulations	
17.	The solution should support the ability to build and test custom lexicon rules from regular expression through the application interface	
18.	The solution should support fingerprinting along with described content	
19.	The solution allows creating policies applicable to individual users or groups as a whole. It should be possible to define exceptions of individual users in a group when the policy is defined for the whole group.	
20.	The same policy should be applicable for the defined content in all possible locations as described above - data at rest, data in motion and data in use.	
21.	The policy should be able to apply different actions when a particular endpoint is within the company network and while it is not connected to the network. The scanning capabilities should not differ in both the modes.	

22.	The solution should provide identical detection capabilities across all threats covered (e.g., for both network and endpoint-based products, and for both data monitoring and prevention and data discovery and protection)	
23.	Support segregated mechanism to define policy and content definition allowing the same content discovery definition to be used by multiple policies and each policy to act on multiple content discover definition	
24.	The solution should provide a SINGLE web based interface for ALL aspects of policy editing and policy management, across all products (across monitoring and prevention and across network and endpoint)	
	Data in Motion	
25.	The entire proposed component for detecting data loss prevention should be in appliance form factor (physical / virtual) for easy management.	
26.	Monitor SMTP including attachments, POP3 including attachments, IMAP, HTTP including file uploads, FTP, IM protocols (AIM, Yahoo, MSN, Google) and properly classify tunnelled IM traffic (HTTP)	
27.	For each of the Internet gateways for SMTP and web traffic dedicated appliances should be provided to monitor and manage any remediation locally without requiring sending the traffic back to a remote server.	
28.	The solution should provide for enterprise license of network DLP for any future addition of Internet gateways for CCI offices located across the India.	
29.	The solution should be able to quarantine any mail that violates DLP policies and notification should be sent to inform for either a self-release of the quarantine mail or by the manager or automated release/drop within a specified time-period.	
	Data at Rest	
30.	Support scanning Windows file systems, Unix File Systems, Storage devices, MS SharePoint, WebDAV, archived and stored emails and RDBMS	
31.	Definable Scan Schedules and Scan windows (ex: pause & resume)	
32.	Ability to meter the scanning speed to ensure optimal resource usage, balance scan load across multiple scanning systems and ability to dynamically commission additional scanning systems to increase scan performance	
33.	Preserve file attributes including 'last accessed' attribute	
34.	The solution should support full and partial text fingerprinting and full binary fingerprinting.	
35.	The solution should support fingerprinting of records stored in a RDBMS. It should be possible to specify only certain columns of the table for fingerprinting.	
36.	The solution should be able to discover fingerprinted data even if	

	the data is not in the same order as the fingerprinted columns.	
37.	The solution should provide mechanism to run the fingerprinting at regular intervals so as to update the fingerprints frequently.	
	Data in Use	
38.	Monitor and Prevent data copied to USB storage devices (thumb drives, CD-ROM's, iPods, Blackberry's, etc.) and other media, copy to File Share, print to attached or network printer	
39.	On-screen, pop-up notification with requirement for end user to acknowledge and justify action	
40.	Identity Aware Policies leveraging Active Directory/LDAP USERS and GROUPS	
41.	The pop-up notifications should have the capability to provide notification in multiple languages including Hindi.	
42.	The matching of content with fingerprints should be done by the agent at the endpoint itself	
43.	Ability to tamperproof the endpoint service on the system and rename the service dynamically based on company policy	
44.	Be able to discover data via fingerprinting on endpoints in disconnected mode	
	Automated Remediation /Data Protection	
45.	Automatically copy, move, encrypt, and quarantine files which violate policy. Automatically Notify the file owner and automatic remediation by applying Microsoft RMS templates	
	DLP Tool defined Role-Based Access and Privacy Control	
46.	Limit incident access for a role by policy, by department or business unit, by country or geography, by severity or remediation status	
47.	Redaction of certain data such as sender identity information (email address, username, etc.) that may need to be kept confidential from certain users to protect employee privacy	
	Incident Handling and Workflow	
48.	The DLP incidents will be managed through the incident management module specified in the GRC section for central incident reporting. However, the DLP solution should also provide the incident management features which can be leveraged as and when required by the administrators	
49.	The solution should be able to provide alerts to the offenders or their managers or the designated owner of the incident via email.	
50.	The solution should provide workflow actions to escalate events and cases	
51.	Ability to export standalone archive of incidents for external review by users without system access.	
52.	The incident assignee should be able to take remedial action directly from the dashboard in the form of delete, shred, copy to secure location, set access control, quarantine etc.	

53.	Sender identity resolution via LDAP and non-LDAP sources of identity information	
54.	View full incident history including all changes and edits to that incident	
55.	Notify the violator and his manager and escalate incident to escalation team or to policy owner.	
56.	All actions taken on an incident should be provided as notification action log.	
57.	The solution should be able to alert/provide a popup to the users as and when they are violating a policy on the end point.	
58.	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content motivated the match.	
59.	The solution should be able to control incident access based on role and policy violated.	
60.	The solution should allow role definitions to NOT have viewing rights to content of the message that violated policy to reduce dissemination of sensitive information of the company e.g. you can define a role “auditor” that doesn’t have the ability to see the matched content, sender, user, or owner, but only the fact that a violation occurred.	
	Reporting and Analytics	
61.	The solution should provide a robust reporting mechanism with reports available out-of-the-box.	
62.	The solution should allow creation of custom ad-hoc reports.	
63.	The reports should be exportable to formats such as HTML, PDF and CSV.	
64.	The viewing of reports should be controllable based on roles.	
65.	The solution should have a capability of emailing reports directly to an individual or a set of individuals without manual intervention.	
66.	The solution should provide a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view	

4.7 Management Information System

MIS will be an integrated information system to provide management with needed information on a regular basis. The information system will be designed to support to the following functions:

- MIS Reports
  - Scheduled Reports
  - Statutory Reports
- Strategic Management
  - Strategic Planning

- Balanced Scorecard
- Operational Management
  - Performance Management / KPI
  - Performance Monitoring
- MIS will also be used across the organization as an information utility to:
  i. Support policy making
  ii. Meet regulatory and legislative requirements
  iii. Support research and development
  iv. Support consistent and rapid decision making
  v. Enable effective and efficient utilization of resources
  vi. Provide evidence of business transactions
  vii. Identify and manage risks
  viii. Evaluate and document quality, performance and achievements.

In the Phase I, the MIS reports will be generated.

The MIS reports will be generated in the various applications and presented in dashboard and Excel- sheets. The following reports would be generated along with other ad-hoc reports that CCI may require.

S. No.	Functionality	Compliance Code
1.	Ability to generate report on Inward Letter Details (Inward Register)	
2.	Ability to generate report on Outward Details (Outward Register)	
3.	Ability to generate report on Department wise File Details	
4.	Ability to generate report on File Status Details	
5.	Ability to generate report on Department wise Pending Inward Letter Details	
6.	Ability to generate report displaying the list of Inward Letters/Internal Notes with no of days being delayed from the actual (based on priority)	
7.	Ability to generate report on Note History and the header should come in all the pages	
8.	Ability to generate report on Department wise Pending Internal Note Details	
9.	Ability to generate report on DAK Details (Inward Register based on the letter type)	
10.	Ability to generate report on Dispatch Details (Inward Register based on the letter type)	
11.	Ability to generate report on Department wise pending files details.	
12.	Ability to generate report on Call book register file details	
13.	Ability to generate report on Brought Forward register file details	
14.	Ability to generate report on Lie Over Till register file details	
15.	Ability to generate report on Stock File Index register file details	
16.	Ability to generate report on Personal Register	
17.	Ability to generate report on Arrear List for section	

S. No.	Functionality	Compliance Code
18.	Ability to generate report on Arrear List for department	
19.	Ability to generate report on Reminder Diary (pending files)	
20.	Ability to generate report on Officer order register	
21.	Ability to generate report on Consolidated Circular register	
22.	Ability to generate report on Stamp account register	
23.	Ability to generate report on Run on Note file register (Personal register approved details)	
24.	Ability to display Organization Structures, Reporting To hierarchy from HRMS module	
25.	Ability to define work flow based on the hierarchy	
26.	Ability to route the workflow based on the assignment given dynamically through the system	
27.	Ability to display the list of Currents Pending for Action based on the login	
28.	Ability to display the list of Files under Movement for Action based on the login	
29.	Ability to navigate to file search screen from dash board	
30.	Ability to navigate to DAK search screen from dash board	
31.	Ability to display the list files pending for the personal register approval based on the login person.	
32.	Ability to display the list of pending files based on the login person.	
33.	Ability to generate statutory reports	
34.	Ability to generate file tracking reports	

4.8 Business Intelligence and Business Analytics

The MIS and DSS will be based on the concepts of Data Warehousing, Data Marts using ETL tools. The system will generate scheduled, statutory and regulatory reports which are currently being produced in various divisions. In addition, the solution will have Business Intelligence tools for query and reporting, multi-dimensional analysis (Online Analytical Processing).

In phase II the tools for Business intelligence applications and analytics would be deployed.

S. No.	Functionality	Compliance code
	Data Warehouse Features	
1.	Enterprise wide data warehouse with ability to provide each organizational department, office or each role within the organization with the needed reliable, consolidated, integrated, actual, and historical information.	
2.	Always on always available access to information	

S. No.	Functionality	Compliance code
3.	Ability to provide the following features as a part of the design environment a. Flexible Data modelling b. Data Acquisition c. Transformation d. Distribution e. Meta Data Management f. Document Management g. User Management h. Administration and Monitoring i. Control of data flow j. Performance Optimization k. Information life cycle management	
4.	Ability to handle/contain both summary and detailed data.	
5.	Ability to seamlessly integrate all operational information.	
6.	Ability to provide each data field with many attributes/characteristics based on which the data can be analysed.	
7.	Ability to enable users to access instantly a variety of immediate data sources and historical records	
8.	Ability to use visualization techniques for data and information presentation	
9.	Should provide option to load full or incremental (Delta) data loads.	
	ETL Tool	
10.	Ability to populate data warehouse.	
11.	Ability to provide Infrastructure to link up process elements, such as sources (selection of data), targets (deployment of results), pre-processing (transformation) and visualization tools, as well as data analysis methods	
12.	Allows for many input and output sources that enable performance management from many perspectives.	
13.	Ability to extract, transform and load data from disparate source systems and perform the necessary transformations to establish a common format	
14.	Ability to load data in different formats like CSV, Flat file, XML, cubes, star schemas, text, images, video etc.	
15.	Ability to allow the historical data to be captured at both transactions level and summarized level.	
16.	Ability to support automatic extraction of data.	
17.	Ability to support import/export of different file formats like Excel and database etc.	
18.	Ability to read and process multiple (heterogeneous) extracts at the same time	

S. No.	Functionality	Compliance code
19.	Ability to support both batch and sequential processing of records	
20.	Ability to support batch and on-line data extraction, transformation and loading	
21.	Available for reporting while the data loading process is going on.	
22.	Ability to provide high-speed data loading with full checkpoint restart and recoverability features.	
23.	Ability to support the load process restart without manual intervention in cases of load failure.	
24.	Ability to support the feature of data loading done in parallel when multiple load jobs are assigned.	
25.	Ability to support conditional logic across multiple fields	
26.	Provide a user-friendly GUI for the users to handle ETL processes, such as: • Modify data feeds • Change of Business logic used for data ETL • Modify ETL parameters • Create, edit and execute a large number of transformation rules	
27.	Ability to expedite the data mapping process from source systems to the DWH objects	
28.	List the source-systems that are compatible with your ETL tool.	
29.	Ability to map/convert source data to the target data structure	
30.	Ability to capture change data (new, change data, deleted data / integration	
31.	Ability to create data marts for different departments, sector wise, area wise, markets - vertical, horizontal etc.	
32.	Ability to Cleanse/Enhance data	
33.	Ability to define and design hierarchies and hold all hierarchy information for any entity	
	End User BI Applications	
34.	Ability to design and provide applications for formatted reporting, ad hoc queries, interactive analyses, information dashboards, and information broadcasting.	
35.	Based on role users, ability to design, deploy, and execute queries, formatted reports, and Web applications.	
36.	Based on role users ability to design and interact with Excel-based business intelligence applications and workbooks.	
37.	Based on role users ability to analyse ad hoc queries and create views of information from various data sources.	
38.	Ability to provide environment for designing, deployment, and execution of information broadcasting, seamlessly integrating business intelligence, knowledge management, and collaboration into a single, blended experience for the end user.	

S. No.	Functionality	Compliance code
39.	Based on role users ability to easily configure business intelligence applications in a visual modelling environment and deploy the results in the net-centric unified access point.	
40.	Based on role ability to view reports for various versions of analysed objects.	
41.	Ability to create custom objects for repeated use	
42.	Ability to create custom formulas using a graphical interface	
43.	Ability to display in different formats like sections, tables, pivots, charts, graphs etc.	
44.	Ability to display multiple result sets in the same document	
45.	Ability to seamlessly merge the dimensions for further analysis for the combined report.	
46.	Ability to selectively hide/show data	
47.	Facility for conditional formatting, based on thresholds or data ranges	
48.	Ability to support custom sorting.	
49.	Ability to create ad-hoc queries and reports for analysis	
50.	Ability to drill across. Ease to slice and dice data	
51.	Ability to provide support for digital dashboards	
52.	Ability to provide a graphical interface with drag and drop features to build reports.	
53.	Ability to store history and statistics of queries executed.	
54.	Ability to schedule a report for execution/refresh and/or distribution	
55.	Ability to allow a user to subscribe to various reports	
56.	Ability to publish reports to a central store for access by different users	
57.	List the mediums of distribution that the tool provides	
58.	Ability to create reports on the desktop available on the web and vice versa	
59.	The reports should be available for time frames like weekly / daily / monthly / yearly.	
60.	The reports should be available in MS Excel or Web (Internet Browser).	
61.	The report data must support the feature of being exported to Excel, ASCII files, PDF and HTML or third party reporting tools	
62.	The reporting feature should support drill down (across reports/within reports), filter & sorting.	
63.	The report should support the view of seeing numbers / graphs or both on a single display.	
64.	The reporting feature should allow for user based templates be created & used for reports.	

S. No.	Functionality	Compliance code
65.	Ability to provide for calculations, filters and exceptions during reporting.	
66.	The reports should be available to users at any time.	
67.	Ability to support the reports to be scheduled to run in batch.	
68.	Ability to notify users when reports have been run.	
69.	Ability to support schedule to run the reports event-based or time based	
70.	Ability to support the feature of delivering the reports to the online users through email, portal, and report server.	
71.	The report should be broadcasted / sent on e-mails.	
72.	Ability to support the feature of alerts to be triggered to management to take proactive decisions.	
73.	Ability to provide for metadata objects be viewed during reporting.	
74.	Ability to allow users drill from the cube to the underlying detail data that fed the cube.	
75.	Ability to provide for saving the report /queries for repetitive execution as and when required by the users.	
76.	The reports to be made available for analysis of historical & consolidated data across systems	
77.	Ability to have the feature of dynamically summarizing data without having to rebuild data.	
78.	Ability to make technical reports available for monitoring the performance of data warehousing system.	
79.	Ability to support management analysis via balanced scorecard for operational information.	
80.	Ability to support visualization of geographic (location based) data on maps	
81.	Ability to provide an easy and intuitive way to detect and analyse • Regional patterns • Resource clustering • Ability to support interactive information analysis on maps • Select and filter (e.g. regions) • Filter (e.g. zone) and drill down (to e.g. substations)	
82.	Ability to generate analytical maps out of the box	
83.	Ability to support with standard interfaces for geographical data such as detailed route maps that can appear in the background of the analytical data	
84.	Ability to support scenarios beyond pure analytical mapping like: • Automatic geo-coding of new resources in the command centre • Perimeter analyses using spatial queries for location searches • Route planning or determining distances for optimization of	

S. No.	Functionality	Compliance code
	routes	
	OLAP	
85.	Ability to create OLAP Database	
86.	Ability to create and process multidimensional cubes	
87.	Ability to update scorecard	
88.	Ability support 15 and odd multi dimensions and each dimension should be capable of over 200 Objects/ characteristics.	
89.	Ability to manage slow changing dimensions	
90.	Ability to run SQL statements	
91.	Ability to run SQL Procedures	
92.	Ability to Process cubes	
93.	Ability to Create PDF Report	
	Data Mining	
94.	Provide Data-mining component integrated with the warehouse	
95.	Ability to provide discovery-driven data analysis	
96.	Ability to provide for Integration of Data Mining Methods with the Data warehousing tool apart for standard support for the following methods	
97.	Ability to use the following methods • Association • Prediction • Classification • Clustering • Summarization • Discrimination	
98.	The ability to use visualization techniques for result presentation	
99.	List the Data mining techniques available in the tool.	
100.	Ability to provide for definition and execution of Data Mining models Process Designer framework	
101.	Ability to provide extended pre-processing abilities to define and prepare (mass) data for training and/or prediction of Data Mining models	
	Meta Data	
102.	Ability to create technical and business meta data	
103.	Ability to propagate changes in the meta data to the warehouse	
104.	Ability to access technical meta data for application development	
105.	Ability to allow users to access business meta data on line for locating information and understanding its characteristics	
106.	Ability to browse through metadata for detailed information on objects	
	Warehouse Administration	

S. No.	Functionality	Compliance code
107.	Ability to deploy DWH	
108.	Ability to integrate tightly with ERP access products	
109.	Ability to export ERP view directly into warehouse environment	
110.	Ability to export short description as labels and long descriptions as notes	
111.	Ability to implement user organization defined archive policies	
112.	Ability to provide for historical data be archived according to user-definable parameters.	
113.	Ability to provide backup capabilities.	
	Security	
114.	Ability to define security policies on a user, permission and object granularity as per user requirements	
115.	Able to support both the Authenticating and Auditing Aspects of the Security	
116.	Able to support security for objects in Data Warehouse	
117.	Able to support the facility of the reports be viewed as per individual user authorization or user defined rule	
	Document Management	
118.	Ability to automatically store scheduled reports in Document Management	
119.	Capturing of document approvals	
120.	Ability to support integration and interfacing with workflow management tools	

4.9 Email and Messaging

An integrated email and messaging application will be installed for enhanced collaboration and communication among users. Officers will be able to connect with each other with services including email, calendars, presence awareness, instant messaging, profiles, status updates, file sharing, and more which is currently not possible with existing mail service.

The application should integrate with NIC email server and will be used majorly for internal communications and workflow integration. Email and messaging solution will access workflow-driven and collaborative business applications that support different business functions.

4.9.1 Technical Specifications

S. No.	Functionality	Compliance code
	Requirement for Mail Server	

S. No.	Functionality	Compliance code
1.	The proposed solution should be compatible on all the operating systems offered by the bidder in the proposed solution including client machines which are most likely window based system.	
2.	Should support for application level clustering and automatic fail over and load balancing services. The clustering should support a minimum of 6 nodes in Active – Active Clustering. Clustering Option may not mandate or make compulsory the use of Shared Disk Storage or common operating systems across the servers in a cluster farm.	
3.	Should provide support for secure login and access	
4.	Should have the capability to do FIELD Level Synchronisation, Selective & Formula Based Synchronisation between Server to Server and Client to Server with a view of being able to propagate documents, mail and directory changes. The synchronisation supported must be Incremental	
5.	Should have inbuilt compression support for Server to Server connections to minimize bandwidth utilization.	
6.	Should be highly scalable and provide for high reliability	
7.	Should provide inbuilt support for event monitors, alarms and statistics reporting. The reports should have a facility to automatically send selective alerts or system errors to a pre-defined Email address.	
8.	Should support Transaction logging for database view indexes.	
9.	Should support Automated fault recovery across different operating platforms.	
10.	Should have integrated support for Instant messaging awareness and chat.	
11.	Policy-based management should provide for centralized, targeted control over user settings, so a change in one place can update users in any scope — from an individual to a group or to an entire organization. Policy Based Management should also provide for control user registration options.	
12.	Policy Based Management should also support Archiving Policies which allow the Administrator to define the server and thresholds for archiving to commence	
13.	Policy Based Management may also Password Expiry and Password Change policies	
14.	Policy Based Management shall come into effect for the thick Client / User at the time of User Registration, User Setup, Every time the user logs on.	
15.	Should Allow administrators to automate notification and distribution of native e-mail client Software Upgrades. This should help to eliminate the need for desk-side visits. Through such upgrades, administrators should be able to configure and assign updates centrally. The mail client can then downloads and install	

S. No.	Functionality	Compliance code
	client updates automatically. The system must allow for a No Touch Upgrade for the Native mail Client.	
	Security	
16.	Should support encryption for all messaging components including local store of data. Local Store encryption shall be customizable for various levels of encryption required. Encryption shall not mean password protection.	
17.	Should provide inbuilt support for digital signature	
18.	Should provide support for simple, flexible administration via a web browser and thick client.	
19.	Should be able to perform Anti-Relay enforcement on incoming connection, allow only the customer's domains	
20.	Should support SSL encryption with 128/168 bit key	
21.	Should provide integrated PKI as a foundation for numerous security features, including: digital signatures and encryption; granular access control -- down to the individual field level; execution control lists; local data encryption; and trust relationships in multi-organization and Extranet applications.	
22.	Should allow multi-level passwords to ensure that no one administrator may have full control of the important user credentials.	
23.	Should provide Reader control at the document/record level to ascertain only selective users may ever be able to search and access such secure and confidential content.	
24.	Should provide flexible delegated administration at the field/granular Level.	
25.	Should provide support for field level security for all messaging components.	
26.	It should offer Hierarchy based delegated administration. It should also support definition of explicit / implicit policy kind of a structure for delegated administration. The delegated administration feature should be OS independent and shall be a function of the Messaging Software and not the OS.	
	Mail Routing Requirements	
27.	The Mails system should have inbuilt utilities to track mail routing process.	
28.	The system should provide scheduled and ad hoc reports.	
29.	Should support Dynamic Least cost based mail routing, connectivity over dial-up / leased line with other mail server.	
30.	The Least cost based Mail Routing should not be completely depend on the DNS service.	

S. No.	Functionality	Compliance code
31.	The Mail Routing system should maintain its own routing table to judge the routing path.	
32.	Should have cluster aware routing process such that if one server fails the Mail router should be able to send the mail to another server in the cluster farm	
33.	Should provide support for graphical mail topology, mapping and monitoring.	
34.	Should provide support and services for protocol like POP, IMAP4, and SMTP etc. along with Web Access support.	
35.	Should be able to perform Anti-Relay enforcement on incoming connection, allow only the customer's domains	
36.	Should provide sender domain validation in DNS (verify connecting domain in DNS)	
37.	Should be able to verify that the local domain user exists in LDAP directory	
38.	Should support for outbound sender and recipient controls (SMTP Rules)	
39.	Should support outbound delivery control based on message priority or count or size	
40.	Should provide support for simple, flexible administration via a web browser. All the functionality of the system including registration of users for Native Client / POP / IMAP/ HTTP etc.	
41.	Should be highly scalable and provide for high reliability	
42.	Network data compression - Network traffic to be compressed at the network layer. This feature requires compression to be enabled on both the client and the server.	
43.	Periodic or per-message notification when the quota is exceeded.	
44.	Should provide for Retention of Mails in case the user reaches his/her quota	
45.	Should support Automatic Clean-up after Message Deletion	
46.	Should support Mail Journaling	
47.	Should have support for both Server Side and client Side Mail Rules to provide controls for message spamming.	
48.	Should support Virus Scanning utilities dynamically scan messages for virus signatures before delivering.	
49.	Should support message store for incoming and outgoing messages	
50.	The system must provide for Server Health Monitoring Tools which provide Analysis and Reports on the health of the server so as to prevent Unplanned Server outages on account of various parameters like Less Memory, Disk space, Processing Power etc.	
	Mail Client	
51.	Welcome Page should be customizable central access point that will allow users to display information they need in the way that	

S. No.	Functionality	Compliance code
	they want.	
52.	Connection wizard - simplifies setup tasks including connecting to POP, SMTP and IMAP servers	
53.	Selective replication & syncronization - Users should create selective replica by selecting databases, documents, views, or folders.	
54.	Data sent over the network can be compressed for more efficient network utilization.	
55.	Allow multiple people to share one Windows OS-based PC. Administrators create multiple-user profiles on a single PC, allowing users to access their personal data while sharing common information	
56.	Roaming user - allow users to have their personal information, Welcome Page, bookmarks, address book, preferences, journal, user dictionary – anywhere they are working.	
57.	Document locking - Soft locks, when a document is being edited, the server copy is protected. Hard locks, to lock a document for an extended period of time.	
58.	Should support multiple archive policies and destinations. Save valuable contents and retrieve them whenever they are needed.	
59.	Viewing, creating, and scheduling calendar entries and meetings.	
60.	Multitasking – Allow users to perform other functions simultaneously.	
61.	Off-line support for all PIM functionality i.e. task management, personal archiving and contact management.	
62.	Ability for the user to change password	
63.	Should allow the user to bring a copy of the server's directory catalogue off-line.	
64.	Allow users to manage another user's calendar. Can compose and accept/decline meeting invitations.	
65.	Can schedule an Instant Messaging meeting directly in calendar and reserve IM resources. It should also provide full scheduling workflow if the meeting needs to be rescheduled.	
66.	Should support Task Assignment	
67.	Should support for Offline support via the Browser	
68.	Should provide for support for Journal Entries	
69.	Support for Drag and Drop Attachments	
70.	Support for Integrated Address Book lookup	
71.	Should support for Mail Box Delegation	
72.	Should be able to create mail with a Signature	
73.	Should be able to set User Mail Preferences like Default Mail Owner, Mail Save Setting, New Mail Notification	
74.	Should provide support for Out of Office Settings	

S. No.	Functionality	Compliance code
75.	Should be able to tentatively accept/draft meetings	
76.	Should provide for Calendar Preferences like Default Appointment Duration, Calendar Entry Type, Auto processing invitations	
77.	Should Print multiple Calendar formats: • Daily • Weekly • Monthly • Calendar List • To-do List • Trifold	
	Additional Requirement	
78.	Multi-Threaded, Multi process for vertical and horizontal scalability.	
79.	Hosted Domain Support.	
80.	Support for setting up Multiple Virtual Domains	
81.	Should redirect HTTP request to user's home Mail server, based on user's home server using LDAP/Address book lookup. Vendors should propose a Reverse Proxy Solution in order to achieve this.	
82.	Should support outbound delivery control based on message priority, count and size	
83.	Should provide for Simplified access to Server Monitoring. Should provide for single-click creation of new database usage, activity, replication, and ACL monitors. Administrators should be able to assess server performance and behaviour in a historical context and in real-time.	
84.	Support for the PKCS#11 standard for smart cards — Smart card support provides additional protection for user credentials. Administrators should be able to enable and disable smart card support on the User Security panel.	
85.	Should provide optional certificate authorization process to the administrators for integrated registration of Digital Keys and Internet Keys. The lower end administrators / designated users should be able to register users without access to the Certifier ID and password	
86.	Any script written by a user (Internal / External) will not execute on the Client Machine unless the same has been certified by the System Administrator	
87.	Should have inbuilt support for Newsgroup Service	
88.	The Vendor should provide upgrade path to allow access to the mail system using Hand held wireless devices.	
89.	The Vendor should provide an option to integrated Audio & Video E-Meeting support with present Messaging deployment.	
90.	The messaging system should have a published API for interfacing with external systems.	
	Workflow Support	

S. No.	Functionality	Compliance code
91.	The messaging system should be extendable to an integrated workflow functionality, i.e. to structure the routing of forms for actions to be followed based on structured maintenance or other messaging related administrative or user mail-enabled applications.	
92.	The messaging system should be extendable to an integrated capability when required to develop, manage, and utilize forms oriented applications, e.g. development of mail enabled "approvals" forms, request forms, and similar functions etc. within the proposed solution.	
93.	The messaging system should be extendable to an integrated approach to support the operation of mail-enabled applications, developed using the provided tools and methodologies, and provide managed access (e.g. to authorized users only) to these applications, e.g. support for mail-enabled applications accessed through the web by personnel from home or from remote locations.	
94.	The workflow engine should provide a tightly integrated security scheme with the e-mailing features	
95.	The workflow functionality should provide the ability to make programs, such as JDBC, ODBC, Java, JavaScript, CORBA, or COM, interface with each other so as to integrate with existing applications and components	

4.10 Human Resource Management System and Payroll

The HR management module will cover all HR aspects from application to retirement. Human Resource Management system (HRMS) will be web based, enterprise wide system which will aim at maintaining integrated information for various functions of the Human Resource department including employee records, recruiting and training, performance analysis and review, administration, leave, attendance, payroll, employee benefits etc.

All employees will have self-service for online access to their personal information and will be able to better track/update the available data.

Also the application will be integrated with Payroll application for salary computation and processing.

Payroll

The payroll module will automate the pay process by gathering data on employee time and attendance, pay particulars, loans and advance recoveries, requested voluntary deductions, ordered recoveries, tax deductions and other voluntary deductions or recoveries, and generating pay cheques, employee tax reports, TDS certificate, salary sheets, ECS Statement, Direct Credit and lists of statements for deductions like life

insurance, co-operative societies etc. It will be closely coupled with the leave management system, attendance system and financial management system. Generate all the general / statutory reports related to employee, attendance/leave, payroll etc. The core features would also include self-service for the following:

- Online access to salary slips via email or self-service portal
- Online access to information on advances, loans etc. via self-service portal
- Online access to TDS Certificate

4.10.1 Technical Specifications

S. No.	Functionality	Compliance Code
	Employee Master	
1.	Ability to identify each employee by unique number	
2.	Ability to capture the name of an employee (First name, Middle name, Last name)	
3.	Ability to capture the employee contact information such as permanent and contact address, phone, email etc.	
4.	Ability to upload the employee photo	
5.	Ability to capture the date of birth of the employee	
6.	Ability to capture the date of joining of the employee	
7.	Ability to update the status of employee such as Probation/ Confirmed/ Resigned/ Terminated/ Suspended/ Deputation/ Retired/ Reemployed.	
8.	Ability to capture the educational qualification details of an employee.	
9.	Ability to capture community details of an employee.	
10.	Ability to capture the gender of an employee.	
11.	Ability to categorize the employee based on the nature of job (Admin/ Officers/ Menial/ others) and cadre	
12.	Ability to define service type for an employee such as full time, part time, contract, deputation employee etc.	
13.	Ability to assign a department or section to an employee.	
14.	Ability to define designation and grade for an employee.	
15.	Ability to define the salary of an employee using standard components (Pay scales) as defined in the Payroll. Earnings and Deductions varies based on field station	
16.	Ability to capture the reporting hierarchy of an employee.	
17.	Ability to capture PAN number, Multiple LIC, Recurring Deposit (RD), Postal Life Insurance (PLI), Society number, Loan Account number etc.	
18.	Ability to store personal information such as date of birth, service start date of an employee, joining date.	
19.	If employee under probation avails leave then the probation period will be increased accordingly. (Manual)	

S. No.	Functionality	Compliance Code
20.	Ability to capture immediate family members including dependent parents and their photo	
21.	Ability to capture the details of publications by an employee	
22.	Ability to maintain the history of all postings	
23.	Ability to define the home town information along with the nearest railway station	
24.	Ability to maintain various declaration details of the employee	
25.	Ability to maintain the nomination details for CPF, Gratuity etc.	
26.	Ability to maintain achievements and awards of the employee and the warnings/punishments and adverse entry against the employee	
27.	Ability to attach Birth certificate of the employee	
28.	Ability to capture the Bank Account details of the employee	
29.	Ability to capture the various deductions like GIS, PPF, LIC, RD, PLI, etc.	
30.	Ability to enable workflow for approval of entries to and amendments to Employee Master Data	
	Organization Structure	
31.	Ability to maintain the details of various sections and departments	
32.	Ability to define various operational wings within the organization	
33.	Ability to maintain the designations and their reporting structure	
34.	Ability to define various roles in the organization	
35.	Ability to assign the employee to their section	
36.	Ability to identify the Head of the Department	
	Manpower Management	
37.	Ability to maintain the Recruitment policy and process all recruitments as per policy	
38.	Ability to initiate the Recruitment process for a vacancy.	
39.	Ability to transfer the staff across different departments and sections.	
40.	Ability to create the selection committee based on the job vacancy	
41.	Ability to capture vacancy details like No. of posts, grade, permanent / temporary /contract /outsource details of pay scale, probationary period etc.	
42.	Ability to differentiate the recruitment process	
43.	Ability to set probation period based on the recruitment process.	
	Recruitment	
44.	Ability to apply online for a particular job vacancy	

S. No.	Functionality	Compliance Code
45.	Ability to create man power requisition with the following details - Number of positions available - No of personnel required - Proposed salary for each position - Approval of requisition	
46.	Ability to identify each candidate by a unique number.	
47.	Ability to capture the name of the candidate	
48.	Ability to capture the candidate contact information such as contact and permanent address, phone, email etc.	
49.	Ability to update the status of candidate such as Applied/Screened/Appeared for Interview/ Selected / Rejected / Waiting / Offer letter sent/Offer accepted/ Offer not accepted.	
50.	Ability to capture the educational qualification details of the candidate.	
51.	Ability to capture community details of a candidate & ability to capture the gender of the candidate.	
52.	Ability to identify the source of the candidate. E.g. Advertisement, employment exchange etc.	
53.	Ability to attach the resume/certificates of the candidate.	
54.	Ability to log mark obtained in the tests/interviews	
55.	Ability to capture selection and screening committee recommendations	
56.	Ability to send call and offer letters by email/ fax.	
57.	Ability to change the offer letter (template) to alter the terms and conditions for particular employee	
58.	Ability to capture the reporting date for a candidate	
59.	Ability to make offer for the selected candidates	
60.	Ability to support the multilevel approval rejection mechanism	
61.	Ability to track/attach the mandatory candidate details, such as - Contact details - Education/Qualification details - Attachment of Certificates - Curriculum Vitae -Mandatory medical check-up form	
62.	Ability to print the contract as per the contract details entered in the system	
	Leave	
63.	Ability to apply different type of leave like Extra Ordinary Leave(EOL), Commuted Leave , Leave Not Due , Sabbatical Leave , Maternity leave, Half Pay Leave.	
64.	Ability to configure eligible number of days for each leave type based on the experience in years and employment status.	
65.	Ability to enter the applicability of encashment for each type of	

S. No.	Functionality	Compliance Code
	leave.	
66.	Ability to configure the number of carry forward days for each type of leave.	
67.	Ability to include or exclude weekend days for leave calculation as per policy	
68.	Ability to capture grace period for each leave type	
69.	Ability to credit Casual Leave and Medical Leave on pro-rata basis.	
70.	Ability to define different level of approval for different type of leaves.	
71.	Ability to update the leave balance of an employee automatically based on the Leave policy.	
72.	Ability to enter the Extraordinary Leave details if the employee is not eligible to take leave or all leaves which are already taken (and the appropriate salary deductions made in payroll).	
73.	Ability to maintain the leave details taken on extraordinary leave for a specific period.	
74.	Ability to transfer the leave when the employee is transferred to other central government office	
75.	Ability to adjust the leave taken (For Leave Not Due) with the future Half Pay Leave availed	
76.	Ability to adjust the leave availed against the 'Leave not due'	
77.	Ability to maintain leave records for each employee	
78.	Ability to allow the employees to access a template of the form, and fill in their request	
79.	Ability to display the employee's respective leave balances, leaves taken and the amount remaining	
80.	Ability to accrue the leave balances automatically based on the leaves taken by employees	
	Loans & Advances	
81.	Ability to apply for different type of loans and advances	
82.	Ability to check the availability of fund in yearly budget for applied loan type. Loans are processed on first come first serve basis. If the fund is not available, the loan is carried forward to next year. Loans can be cancelled	
83.	Ability to define maximum amount for each type of loan	
84.	Ability to define the number of loans which can be taken for a given period or during the entire tenure for each loan type.	
85.	Ability to capture the following details, interest Amount, Lead time for first instalment for each loan.	
86.	Ability to capture the loan details such as Employee personal Information, Loan amount, Percentage of interest, and Start date of deduction. Agreements to be maintained manually (not in scope of the system)	

S. No.	Functionality	Compliance Code
87.	Ability to define eligibility criteria based on salary (Basic + DP), Cadre wise	
88.	Ability to define number of instalment for each loan type with in which the employee has to repay the loan	
89.	Ability to release the loan amount in different stage of work completion for certain loan type like housing loan.	
90.	Ability to instruct the payroll to deduct the loan instalment amount from the salary	
91.	If the employee wishes to pay the balance amount then the system should have the provision to capture the details and update the payroll.	
	Assessment	
92.	Ability to identify the list of Employee to be assessed on a given period.	
93.	Ability to track all the documents submitted by the employee during assessment initiation.	
94.	Ability to capture the self-assessment based on Technical & Non-Technical category.	
95.	Ability to maintain history of the changes in the salary structure of an employee. Option to capture the effective date of the change.	
96.	Ability to define different type of Assessment	
97.	Ability to get Confidential report from the Reporting Officer with appropriate details.	
98.	Ability to get promotion recommendations from HOD.	
99.	Ability to capture details of the interview conducted for an employee based on definition.	
100.	Ability to instruct the payroll to change the pay band of the employee based on the promotion or increment given after the assessment	
101.	Ability to capture next assessment date for the employee who got only increment and not promotion.	
102.	Alert has to be sent to the employees before every assessment	
	Employee Separation	
103.	Ability to define various type of Retirements such as Superannuation Retirement, Voluntary Retirement, Compulsory Retirement	
104.	Ability to define the age limit, years of service for each retirement type, class and nature of job (Manual)	
105.	Ability to get no due certificate from the employee who are in the process of separation	
106.	Ability to define various type of benefits such as Death cum Retirement Gratuity (DCRG), Commutation (Optional), Contributory Provident Fund , Leave Encashment, TA on retirement.	

S. No.	Functionality	Compliance Code
107.	Ability to calculate date of superannuation for the employee based on date of birth.	
108.	Ability to have commutation benefits	
109.	Ability to pay TA as a benefit to the retiring employee	
110.	Ability to define rule to avail commutation benefits. For example: Employees who have served more than 10 years are eligible for commutation.	
111.	Ability to send alert to the retired person to produce medical certificate	
	HRMS Reports	
112.	Ability to generate the service book of the Employee	
113.	Ability to generate reports showing the details of the Employee like Id, name, designation, email id, qualification, department ,nature of jobs, gender and grade	
114.	Ability to generate the short listed candidate list report.	
115.	Ability to generate Call letters for the eligible candidates	
116.	Ability to generate Offer letters/Appointment letters for the selected candidate	
117.	Ability to generate report showing the list of selected candidate with details of joining etc. for a selected period	
118.	Ability to generate report showing the details of the Home Town Declaration of the selected employee	
119.	Ability to generate a leave detail report for a Department / Employee with the details like Employee Id, Name, Leave type, start date and end date of the leave.	
120.	Ability to generate leave summary report with the details like Employee Id, Name, Eligible number of days, Number of days availed, Balance for each leave type	
121.	Ability to generate the Extraordinary Leave report for the specified period/ Employee.	
122.	Ability to generate Confidential Report for the employee	
123.	Ability to generate Self-Assessment for the employee	
124.	Ability to generate the Performance Assessment report	
125.	Ability to generate Assessment Result Letter of the selected employee	
126.	Ability to generate report showing Increment list of all the employee for the selected period	
127.	Ability to generate Seniority list report based on designation across the departments/section.	
128.	Ability to provide a view that summarizes all Career changes of an employee for a defined period	
129.	Ability to generate Reports for Loans and advance.	

S. No.	Functionality	Compliance Code
130.	Ability to generate report showing the details of the vehicle loan applied by the selected employee	
131.	Ability to generate report showing the details submitted by the employee for the property loan	
132.	Ability to generate report showing the list of employee who are going to retired in the selected period	
133.	Ability to generate settlement report to an employee.	
134.	Ability to generate service certificate, relieving order, no due certificate etc.	
	Payroll Processing	
135.	Ability to define the relationships (formula) between various salary components. DA, HRA, CCA are components of the salary that dependent on Basic.	
136.	Provision to define slabs for required components of the salary.	
137.	Ability to define Earnings and Deductions	
138.	Provision to define different pay band that depend on designation, grade and location	
139.	Each pay band should capture the minimum amount, maximum amount and grade pay	
140.	Ability to define pay band for an employee which may or may not be the same that defined for his Designation, grade and field station	
141.	Ability to support different periods for the pay band	
142.	Ability for disbursement of salary either through bank or by cash/cheque	
143.	Ability to change salary based on the promotions for the employee. (When a change in pay band occurs)	
144.	Ability to define rules for increments such as increments once in a year on reaching the maximum limit in a pay band without getting promoted.	
145.	Ability to make changes in salary based on the yearly increment, ad hoc increments, etc.	
146.	Provision to define salary for officers who have been deputed by external agencies for a specific period of time	
147.	Provision to handle pensions for employee under Superannuation based on configuration	
148.	Provision to define ad-hoc payments to all employee such as pay arrear, bonus etc.	
149.	Provision to handle Leave encashment only during superannuation	
150.	Provision to define salary components that are constant for all employees.	
151.	Provision for disbursement of arrears and advances either through bank or by cash	

S. No.	Functionality	Compliance Code
152.	Ability to segregate and display the deductions as Adjustments and Remittance	
153.	Ability to deduct, income tax and professional tax for the employee	
154.	Provision of disbursement of Gratuity	
155.	Ability to instruct the payroll to deduct the exceeding amount at TA etc.	
156.	Ability to amend Employee salary information in either as individual entries (or) jointly as a group based on the criteria	
157.	Ability to add / delete an allowance to an employee	
158.	Ability to view the back dated payroll entries	
159.	Can system define exclusion of pay elements to pre-defined criteria (e.g., consultants not eligible for allowance)	
160.	Ability to define a payroll earning or deduction as recurring or non-recurring for each employee	
161.	Ability to maintain multiple payment components on the system	
162.	Ability to define bank details of employees which can be assigned to the employee payroll	
163.	Ability to capture the PDS (Postal Development Scheme) details	
164.	Does the system has the provision to add a new earning/deduction to the existing pay band	
165.	Does the system has the provision to delete a earning/deduction from the existing pay band	
166.	Does the system hold the history of all the previous data generated with respect to payroll	
	TDS	
167.	Provision to calculate TDS on processing the payroll	
168.	Provision to handle arrears with retrospective effect.	
169.	Provision for TDS and other Income tax related deductions such as professional tax	
170.	Provision to allow employee to give tax exemption declarations under various heads like Section 80C , 80CC, 80U etc.	
171.	Ability to adjust the tax declaration and view the tax payable	
172.	Ability to adjust the Tax declaration within the specified time period (Time period need to be parameterized) ex: they can adjust only up to mid of the financial year	
173.	Provision to take an employee tax declaration into consideration, check it against the eligible limit for that head, as specified by the Government, and include the exemption while calculating the Tax.	
174.	Flexibility to deduct taxes in required months and disallow deduction during others at the time of Pay-slip generation.	
175.	Ability to deduct the Professional Tax in specific months	
176.	Ability to calculate the HR Exemption as a minimum of HRA or sum	

S. No.	Functionality	Compliance Code
	of Actual House Rent and Housing Loan Interest (HLI).	
177.	Ability to set tax deduction frequency based on the field station for certain tax deduction like Professional Tax	
	Payroll Reports	
178.	Ability to display the Scale of Pay as Minimum Amount, Increment Amount, Maximum Amount, Running Increment, Saturation Amount based on the designation	
179.	Provision to generate pay-slip and print	
180.	Ability to generate consolidated Deductions Employee-wise Report	
181.	Ability to generate Form 16,Form 24Q Report	
182.	Ability to generate Pay Structure Report for the selected designation	
183.	Ability to generate Investment Proof Report	
184.	Ability to generate Salary History Report for the selected employee	
185.	Ability to generate Acquaintance (Bank Interface)Report	
186.	Ability to generate Individual/Consolidated deductions field station wise Report	
187.	Ability to generate a yearly Statement for Provident fund with interest	
188.	Ability to generate Individual/Consolidated Pay Abstract	
189.	Ability to generate the list of employee for each pay period with the following information, employee id, and employee name, account number, net pay.	
190.	Ability to generate contract employee payment report for the selected duration	
191.	Ability to generate the pay salary certificate report	
192.	Ability to generate report showing the earning, deduction and tax declaration detail of the employee (Tentative & original)	
193.	Ability to generate special provident fund work sheet with entire deduction details and calculations	
194.	Ability to generate Provident Fund Broad Sheet (Work Sheet)	
195.	Ability to generate report showing the Drawl of Arrear Dearness Relief	
196.	Ability to generate report showing the New Pension Scheme Deduction Statement	
197.	Ability to generate comparison report between the actual salary paid and the proposed salary (salary component)	
198.	Ability to generate a consolidated pay report for regular/non regular/contract employee respectively	
199.	Provision to generate reports for questions related to Ministry related to pay like actual on the pay, projected estimation for pay, vacancy details etc.	

S. No.	Functionality	Compliance Code
	Employee Self Service	
200.	Able to allow employees ▪ To check leave balance and apply for leave ▪ To find out eligibility and apply for LTC, Housing Accommodation loans and advances etc. ▪ To check GPF loan entitlement and apply for GPF loan on line ▪ To view their own master data of service book via intranet/internet. ▪ To view monthly payroll result (follow on monthly slip) ▪ To check loan and advance balance ▪ To check balance GPF loan ▪ Able to allow employees to electronically submit their own personal data, address, telephone number, e-mail address and fax number etc. ▪ Able to allow employees to electronically enrol training courses, view training history and inquire on training courses available ▪ To check audit objection entries ▪ To apply for No Objection Certificate (NOC) ▪ To apply for No Dues Certificate (NDC)	
201.	The system security should be able to prevent users from viewing or changing other employees records or certain information contained in their own records	
	Employee Claims and Reimbursements	
202.	Ability to capture the Medical bill claims.	
203.	Ability to capture the various types of allowance.	
204.	Ability to capture the advance and settlement details of the allowances.	
205.	Ability to pass the bill on to the finance for the allowance being paid.	
206.	Ability for built in work flow definition for directing the allowance to the respective authority.	
207.	Ability to view the leave balance while applying for LTA.	
208.	Ability to deduce EL while applying for LTA.	
209.	Ability to automatically calculate the DA in LTA record based on the applicant's details.	
210.	Ability to maintain the history of all the allowances paid.	
211.	Provision to capture the Telephone Reimbursement.	
212.	Provision to capture the General Reimbursement.	
213.	Ability to capture the contingency allowance.	
214.	Ability to generate the salary advance.	
215.	Ability to assign a GL Account by claim type.	

S. No.	Functionality	Compliance Code
216.	Ability to identify the advance settlement defaulters list.	
217.	Ability to generate the medical bills of the employee.	
218.	Does your system have the provision to generate report for the various types of allowances like LTA, TA, Telephone, Contingency, etc.	
219.	Ability to generate report by various measures like • Time period • Employee • Claim Type • Claim Number • Status of the claim like draft, submitted, approved	
220.	Ability to transfer the advance to be deducted from salary after a certain period as set by the user.	
221.	Ability to capture travel requisitions from employees.	
222.	Ability to forward the requisition to the personnel concerned through workflow.	
223.	Ability to update accounts for the payment when a ticket is booked for travelling.	
224.	Ability to provide information about the eligibility of the employee when a requisition is received from the person.	
225.	Ability to provide information about travel advances provided to the employee pending to be settled prior to authorization of the fresh requisition.	
226.	Ability to provide information about travel advance requested by the employee to be approved by the personnel concerned.	
227.	Ability to alert the personnel concerned about travel advance pending with the employee when processing a fresh advance.	
228.	Ability to post an accounting entry for the travel advance when the request is approved.	
229.	Ability to allow the employees to attach the bills with respect to the medical treatments.	
230.	Ability to have the provision to recover the advance from the defaulters either as monthly instalments from their salary or as cash receipts	

4.11 Front Office Management

The Front Office Management module will help CCI Administration Division in the following ways:

- Manage Security Desk
- Central directory of all officials Name, telephone and their room location etc.
- E-record of passes issued and their expiry date
- Record Visitor appointments given by officials;

- View appointments at desk and issue passes with photo capture.
- Confirmation by the official visited with time and date.
- Tracking of Gate passes

4.11.1 Technical Specifications

S. No.	Functionality	Compliance code
1.	Should be able to define roll of security personnel and the seat attendant on a day and at a time	
2.	Should provide directory of all officials Name, telephone and their room location etc.	
3.	Should provide Directory of emergency numbers	
4.	Should have facility to click dial officials and emergencies from desktop	
5.	Should have functionality to generate E-Record of gate passes issued and their expiry date	
6.	Should have functionality to integrate with calendar for synchronization of appointments given by officials for viewing at desk and pass issuance	
7.	Should have functionality to issue Entry Pass for visitors entering premises with photo capture.	
8.	Should have functionality to confirmation by the official visited with time and date.	
9.	Should have functionality for Gate passes issued for taking out equipment or material	
10.	Gate Pass collection and checking against gate pass issued records for material / equipment going out of premises.	
11.	Checking term passes against– smart card, if feasible, for auto recording of entry time and exit time on a day.	

4.12 RFID based Library Management System

Library Management system (LMS) will be a web based system which will help to automate the vital activities of Library. The LMS Solution will be integrated with RFID for easy access and retrieval of any item from the Library.

The functionalities of the LMS would include acquisition, cataloguing, circulation, OPAC, serials, administration, and stock verification, inter library loan, accessioning, masters, MIS reports, etc. An online public access catalogue (OPAC) facility will provide speedy retrieval of any kind of document, file etc.

RFID (Radio Frequency Identification) system should be integrated for tracking of materials throughout the library, including easier and faster charge and discharge, inventorying, and materials handling. RFID systems should have the ability to scan books on the shelves without tipping them out or removing them. A hand-held inventory reader will be moved rapidly across a shelf of books to read all of the unique identification information.

Self-check-out / check-in is also feasible with the deployment of a check-out desk and a check-in desk where the readers can just enter their credentials and RFID reader will automatically detect the book being checked-out or checked-in.

4.12.1 Technical Specifications

S. No.	Functionality	Compliance code
	General	
1.	E-Bin for each shelf	
2.	Use of Smart Cards / RFID	
3.	Handling PDF files – organise, search and retrieve.	
4.	Barcode based auto recordings of issuance and return (when procured and operationalized).	
5.	Search facility of indexes, abstracts and text.	
6.	E-journal and e-books management components.	
7.	Matching reader / member profiles with articles, journals and books receipt.	
8.	Interfaces with other institutional libraries – protocol authentication	
	Facilities	
9.	Search for catalogue record via any indexed field	
10.	Alphabetical listing of entire catalogue	
11.	ISBN validation	
12.	'Fiction' checkbox for Fiction / Non-Fiction borrowing statistics	
13.	List of Publishers with ISBN prefix provided	
14.	'Do Not Index' option for restricted stock	
15.	Recall facility	
16.	Reservation history facility	
17.	Current Reservations information	
18.	Date facility (e.g. item expiry, renewal, review etc.)	
19.	Composite / Included catalogue record facility for multi-volume works	
	Report Generation Facility:	
20.	The following queries will be on line: • No of books issued in a given period. • New arrivals during a period • Selective dissemination of information about new arrivals according to interests of members – auto triggers. • List of books for physical verification • History of books issued – how many times and by whom. • Reminders for subscribed serials where due and not received. • Reminders to institutions of which CCI is a member and	

S. No.	Functionality	Compliance code
	magazines / journals are received as membership benefits.	
	Circulation	
21.	circulation (lending materials to patrons and receiving them back)	
	Borrower	
22.	Numerous borrower categories with library-defined limits and rules	
23.	Borrower records accessed by name, number and/or barcode	
24.	Full history held for each borrower and item	
25.	Extensive Statistical borrowing reports	
26.	Messages for borrowers	
27.	Automatic loan/reservation stops for borrowers	
28.	Quick cataloguing while check out	
	Issue and Return	
29.	Bar-code readers and accessions (when procured and operationalized)	
30.	Due dates automatically calculated	
31.	Validity check on barred borrowers	
32.	Different book loan periods possible for same items	
33.	Checks items for reference copies	
34.	Quick cataloguing of items and addition of borrowers	
35.	Copy number of loan recorded when more than one	
36.	Checks for reservations	
37.	Checks for overdue/fines	
38.	Messages about specific items e.g. check for CD with book	
39.	Timed loans (short loans)	
	Renewals	
40.	Renewals possible without discharge and reissue	
41.	Record of renewals for each current loan	
42.	Ability to limit renewals	
43.	Renewal by block or individually	
44.	Option to bar renewal of reserved items	
45.	Book Reservation	
46.	Priority reservations	
47.	Printable list of reserves for each item	
48.	Printable list of reserved items	
49.	‘Cancel reservation’ can be undertaken by borrowers	
50.	Printable reservation notifications	
51.	Reservation availability notified when borrower ID entered	

S. No.	Functionality	Compliance code
52.	Automatic trap on reserved items upon return	
53.	Recall reserved items facility	
	Cataloguing	
54.	Classifying and Indexing	
	Data Entry Controls	
55.	User-defined list of media types	
56.	Multi-value Subject/Classification Index	
57.	Author Authority File	
58.	User-defined list of personal roles (e.g. author, editor etc.).	
59.	Multiple Corporate Authors	
60.	Multiple Series field	
61.	Unlimited Keywords with authority file and thesaurus control	
62.	Multiple Languages field	
63.	Copy Information	
64.	Accessioning of copies direct from Catalogue Record	
65.	User-defined list of locations	
66.	User-defined list of accession statuses	
67.	Due Date of Loaned/Ordered items displayed details	
	Desirable information	
68.	Current Price information	
69.	Source of Data information	
70.	Date Ranges information	
71.	User-defined fields	
72.	**Serials** (tracking magazine and newspaper holdings)	
73.	Unlimited number of copies of a given issue	
74.	Capability to search for an issue by keywords	
75.	Predict Next due date	
76.	Reader List	
77.	Bind Serials	
78.	Serial Receipts	
79.	Serial Cataloguing	
80.	**Acquisition:** This process would cover purchase of books, e-books, subscriptions, journals- hard copy, e-journals and the related activities of receipts, budgeting and generating reports on orders and funds and handling standing orders and periodicals.	
81.	ordering, receiving, invoicing materials	
	Interfaces	

S. No.	Functionality	Compliance code
82.	the OPAC (public interface for users)	
83.	GUI Interface	
84.	For Patrons	
85.	For Staff	

4.13 Forensic Analysis

Computer Forensic software tool should be able to gather, analyse and present electronic data that can have a bearing on the case in hand.

It will be used by DG Office officials to help them identify and ferret out data that is hidden using steganography, encrypted, deleted, protected etc. It should have the ability to recover deleted, hidden or damage data from disk drives etc.

4.13.1 Technical Specifications

S. No.	Functionality	Compliance code
1.	Ability for Email analysis	
2.	Ability to analyse the registry	
3.	Ability to decrypt files	
4.	Ability to crack passwords	
5.	Ability to recover deleted, hidden or damage data from disk drives	
6.	Ability for Cross-drive analysis to correlate information found on multiple hard drive	
7.	Ability to integrate with volatility memory (RAM) to easily list processes, open connections and files, loaded libraries, etc.	
8.	Ability to identify and decipher the data stored in steganography	
9.	Ability to analyse the metadata	
10.	Ability to analyse and recover information from mobile devices such as mobile phones, smart phones, GPS navigation tools and tablet computers	
11.	Ability to logically examine direct communication with the device operating system	
12.	Ability to physically examine (bypassing the operating system and dumping available memory)	
13.	Ability to recover more deleted information such as messages, images, files and call records etc.	
14.	**Acquire from Almost Anywhere** : Acquire data from disk or RAM, documents, images, e-mail, webmail, Internet artefacts, Web history and cache, HTML page reconstruction, chat sessions, compressed files, backup files, encrypted files, RAIDs, workstations, servers, and with Version 7: smart phones and	

S. No.	Functionality	Compliance code
	tablets.	
15.	**Forensically Sound Acquisition**: Ability to produce an exact binary duplicate of the original drive or media, and then verify it by generating MD5 hash values for related image files and assigning CRC values to the data. These checks and balances reveal when evidence has been tampered with or altered, helping to keep all digital evidence forensically sound for use in court proceedings or internal investigations.	
16.	**Advanced Analysis**: Ability to Recover files and partitions, detect deleted files by parsing event logs, file signature analysis, and hash analysis, even within compounded files or unallocated disk space.	
17.	**Improved Productivity**: Ability to preview results while data is being acquired. Once the image files are created, examiners can search and analyse multiple drives or media simultaneously.	
18.	**Automated de-NISTing Capabilities:** Allowing user to easily de-NIST their evidence, eliminating thousands of known files from their evidence set. This reduces the time and amount of data that needs to be analysed significantly.	
19.	**Multiple File Viewer Support**: Ability to view hundreds of file formats in native form, built-in Registry viewer, integrated photo viewer, see results on a timeline/calendar.	
20.	**Automatic Reports:** Ability to export reports with lists of all files and folders along with detailed list of URLs, with dates and time of visits. Provide hard drive information and details related to the acquisition, drive geometry, folder structure, etc.	
21.	**Actionable Data**: Ability to create a comprehensive report based on identified relevant information for presentation in court, to management or stakeholders in the outcome of the investigation.	

4.14 Inventory and Asset Management

The Inventory & Asset Management module will be used for inventory management, vendor management, accounting management, purchase management, receiving management, reports, etc.

Inventory and Asset management solutions will maintain records of all consumable and durables assets, including IT assets.

Asset management solution should be integrated with RFID tracking system.

Solution should be integrated with Finance application for calculation of asset depreciation.

Purchase

S. No.	Functionality	Compliance Code
	Supplier	
1.	Ability to capture the Supplier Code, Contact information and contact person details.	
2.	Ability to maintain each supplier terms and default mode of payment	
3.	Ability to maintain currency of payment and mode of payment of a supplier	
4.	Ability to capture the Bank account Number and bank details of a supplier	
5.	Ability to capture the credit limit and credit account of a supplier	
6.	Ability to maintain list of both registered as well as unregistered suppliers	
7.	Ability to capture the tax code for a supplier	
8.	Ability to capture Blacklisting of supplier	
	Material Master	
9.	System should maintain list of material.	
10.	System should be able to maintain Material code, description, type and Category (consumables and Non Consumables)	
11.	System should maintain the unit cost of the material	
12.	System should maintain the list of suppliers who supplies the material	
13.	System should maintain the default unit of measurement for a material and should be able to assign alternate unit of measurement	
14.	System should be able to capture Re-order Level and maintain Minimum Stock accordingly	
15.	System should be able to capture whether the material is an asset or other type of item.	
16.	Ability to classify the items under category	
17.	Ability to capture and maintain details of Warranty, AMC, Service Assistance details, Phased out Product etc.	
	Tender Process	
18.	Ability to capture the details of the indent that is identified by an unique number	
19.	Ability to allow to add more than one material to an indent	
20.	Ability to have the provision for the indent to undergo various status changes like created, submitted, approved, closed, rejected and cancelled.	
21.	Ability to have the provision to notify the appropriate persons for the indents waiting for approval.	
22.	Ability to capture the remarks by different approvers.	

S. No.	Functionality	Compliance Code
23.	Ability to validate for the availability of sufficient funds from the budget for an indent	
24.	Ability to set up Types of Tender and the days required to respond for that type of Tender.	
25.	Ability to capture tender details like Title, Place of execution, Mandatory documents, Earning money deposit, etc.	
26.	Ability to associate a tender to more than one indent.	
27.	Ability to capture response from more than one suppliers	
28.	Ability to capture the Response number, date, supplier details, contact person for a quotation	
29.	Ability to capture advance requested for supply of materials	
30.	Ability to capture Indian currency, foreign currency amount and exchange rate	
31.	Ability to capture the Guarantee/ Warranty and Validity details	
32.	Ability to capture the Quotation Number and Quotation Date details.	
33.	Ability to upload data to Tenders.gov.in as per the required format.	
	Purchase Order / Work Order	
34.	Ability to provide a link for the Purchase Order to the quotation received	
35.	Ability to capture the details of the purchase order like order number, date, document type, raised by, department, project, payment mode, dispatch mode, payment currency, store, Item, quantity, amount, the terms of payment, delivery date and special terms and conditions if any.	
36.	Ability to capture taxes like Sales tax, Service tax, Customs duties, Central service tax, Insurance charges, Packing charges.	
37.	Ability to capture tax exemption details that are applicable for Custom duty, Excise duty etc.	
38.	Ability to map a material to a GL Account and ability to capture the supplier creditor GL account	
39.	Ability to capture the delivery details of the materials in the generated Purchase Order	
40.	Ability to map the budget fund to the Purchase Order	
41.	Ability to amend the Purchase Order	
42.	Ability to have the provision for the approver to view Purchase Order report in Purchase Order Approval screen	
43.	Ability to create work order for the bidder who has quoted high	
44.	in the process of availing any service, does your system has the disposal of materials or purchase of nonstandard items	
45.	Ability to capture work order number, name of the work, date, document type, raised by, department, store, vendor details, unit	

S. No.	Functionality	Compliance Code
	price and amount, terms and conditions if any	
46.	Ability to support creation of multiple types of purchase requisition transaction based on types of items/department	
47.	Ability to support multiple PO for a single reference	
48.	Ability to create multiple work flow/processes/types of purchase order to control different types of purchases: • Foreign purchases • Local purchases	
	Reports	
49.	Ability to provide a list of all funds disbursed for a period by: • Account • Vendor	
50.	Ability to provide an on-line query by: • Vendor • Voucher • Due date	
51.	Ability to provide a report showing total payments to a vendor in a period	
52.	Can your system generate the following reports for a given period / date range: • Aging of payables: • Payment register • Payments overdue listing	
53.	Ability to generate withholding tax report: • Vendor • For a given period	
54.	Ability to control the Invoice amount not to exceed the limit of the PO (With certain defined variance)	
55.	Can your system check and control if the invoice amount is greater than the receipt amount	

Stores

S. No.	Functionality	Compliance Code
	Stores / Inventory	
1.	Ability to support variable item code	
2.	Ability to maintain the following: • Item/Product classification (laboratory, spares, stationary, etc.) • Number of classification levels supported • Items of different origin	

S. No.	Functionality	Compliance Code
	• Can your system support following unit of measure features: • Base UOM for an item/product • Transaction UOM (for purchase, sales) • Conversion with decimal features	
3.	Can your system integrate to GL accounts based on item code, item groups	
	Stores Voucher	
4.	Ability to identify the indent by an unique indent number	
5.	Ability to capture the details of the Indent like Date of Indent, Item code, Description, Quantity requested, Quantity Delivered, Required Ability to record Date of delivery, indenter etc.	
6.	Ability to maintain the status of the indent	
	Stock Register / Auditing	
7.	Ability to maintain the stock registers.	
8.	Ability to capture the details of defected items and provision to maintain the purchase return details	
9.	Ability to make adjustments to inventory after physical audit.	
10.	Ability to classify the materials on the basis of electrical, electronic etc.	
	Goods Receipt	
11.	Ability to maintain goods receipt.	
12.	Ability to capture the details of goods receipt such as Goods Receipt number, date, supplier details, Delivery challan number and date, Part/Full supply should be captured as part of goods receipt in addition.	
13.	Ability to associate goods receipt to Purchase Order number	
14.	Ability to capture details of materials like code, description, quantity received, quantity accepted should also be captured	
15.	Ability for quality checking process for the received items	
16.	Ability to generate receipt of items internally returned by the employees along with details like receipt no, date, employee details, department, stores, item, description, quantity and reason	
	Issue Material	
17.	Ability to capture details of issue of goods like Goods issue number, date, issued by, issued from store, received by and indent number	
18.	Ability to record and maintain details of Material like code, description, requested quantity, quantity issued and quantity pending should also be captured.	
	Stores Receipt	
19.	Ability to maintain Store receipt/Store Inward. Store Receipt	

S. No.	Functionality	Compliance Code
	number, date, supplier details, Delivery challan number and date.	
20.	Ability to associate Store Receipt/Store Inward to Store Return/ Gate Pass number.	
21.	Ability to automatically update the quantity after the return of the materials	
	Invoice	
22.	Ability to maintain invoices that have been received from suppliers.	
23.	Ability to maintain system generated invoice no, date, supplier Invoice no, invoiced by, Item Code, Item description, Unit cost, Total cost, quantity received, quantity rejected, quantity invoiced, Taxes, Location, Address and Remarks.	
24.	Ability to associate Invoice to a goods receipt.	
25.	Ability to Post invoice data to financial system.	
26.	Ability to associate Invoice number to purchase order number	
27.	Ability to capture the freight charges and clearance charges	
	Report	
28.	Ability to maintain a perpetual Stock Ledger	
29.	Ability to prepare a stock reconciliation statement on a daily basis	
30.	Ability to generate a stock report as on any date, based on the pre-determined categories	
31.	Ability to generate a report on the adjustments to inventory arising from Physical verification	
32.	Ability to provide stock aging report	
33.	Ability to show up reports based on stock value	
34.	Ability to generate report on adjustment type of transactions	

4.15 Event Management

Event Management system will be used for facility scheduling, function coordination and seminar management. The system should prepare an accurate plan and keep all elements of workflow of the team/division in coordination with each other, so that different members of team can work coherently using shared and coordinated event calendar, tasks, goals and objectives. The software should give users the ability for:

- Scheduling events
- Managing events or recurring events
- Online registrations
- Sending invitations
- Speakers Database
- Reporting

4.15.1 Technical Specifications

S. No.	Functionality	Compliance code
1.	Ability to create Electronic File Folders –storing all documents and other forms of written communication related to a particular event in an electronic file folder.	
2.	Ability to upload contents in Electronic Folders and share the contents via emails etc.	
3.	Ability to create Event Diaries for storing notes and activity updates, to-do lists, meeting summaries and other information a team needs in order to stay on the same page so that one department knows what the other department is working on.	
4.	Ability to copy Event Templates to duplicate events to new dates and times without the need for additional data entry to save time by copying previous events or creating event templates to use in the future.	
5.	Ability to enable Online Registration integrated directly with event management processes, so registration data is shared directly with event management data.	
6.	Ability to design –customizable badges. With attendee's name and event.	
7.	Ability to control the number of attendees who can register, or simply capture interests for determining space requirements.	
8.	Registrants enter all their own information at their convenience using a standard web-browser interface	
9.	Generates a professional appearing confirmation letters and invoices confirmation letters and invoices	
10.	Schedules follow-up actions and call backs.	
11.	Automatic duplicate checking, spell checking and zip code lookup.	
12.	Registration and tracking of seminar and conference attendees.	
13.	Produces customized reports that can be tailored by the user.	
14.	Uses Relational Data base Management System.	
15.	Uses a sophisticated backup system in multi-user environment to safeguard data.	
16.	User defined pop-up list.	
17.	Sophisticated Password System for multi-level access.	
18.	Event Registration	
19.	Staff Scheduling	
20.	Speaker & Abstract Management	
21.	Document Management	
22.	Event Management & Coordination	
23.	On-site Registration Check-In and Ordering	
24.	Audience Participation & Surveys	
	Meeting	
1.	Ability to create multiple types of meetings	

S. No.	Functionality	Compliance code
2.	Ability to maintain accessories that required to meeting	
3.	Ability to view meeting room details	
4.	Ability to form person groups	
5.	Ability to support to conduct various kind of meetings	
6.	Ability to maintain meeting agenda	
7.	Ability to create meeting events	
8.	Ability to capture the participant details of meeting	
9.	Ability to maintain MOM of the Meeting	
10.	Ability to create, update or delete meeting rooms with the following attributes: • Room code and description • Room capacity • Accessories available like projector, system etc. • Location of the meeting room	
11.	Ability to check for the availability of the room	
12.	Ability to update the room occupancy details, once it is booked	
13.	Ability to display the dashboard for approving authority	
14.	Ability to schedule event through scheduler	
15.	Ability to modify event through event scheduler	
16.	Ability to delete event through event scheduler	
17.	Ability to reschedule the meeting	
18.	Ability to send alert to participant while reschedule the meeting	
19.	Ability to modify the participant details of meeting	
20.	Ability for requesting additional accessories for meeting	
21.	Ability to cancel the meeting	
22.	Ability to add the external participant to meeting	
23.	Ability to add the meeting rooms	
24.	Ability to activate or inactivate the meeting rooms	
25.	Ability to generate report to display complete meeting details	
26.	Ability to generate report to display list of meetings scheduled	
27.	Ability to generate report to display list of meetings completed	
28.	Ability to modify the action items	
29.	Ability for a common window to view all the details related to meeting module.	

4.16 Finance and Accounts

The Finance and Accounts module will take care of various functional and management aspects related to finance and accounting activities of CCI. The F & A module will record, monitor and maintain all accounting and financial transactions of CCI. The module will consist of finance, planning & budgeting, accounts, audits, etc. The module should provide:

- Instant access to accounting information

- Easy document/report production.
- Ability for taxes to be computed automatically
- Efficient budget tracking.
- Reporting

The package shall be integrated with HR, Payroll modules and Inventory and Asset Management modules.

4.16.1 Technical Specifications

S. No.	Functionality	Compliance Code
	Chart of Accounts	
1.	Ability to define chart of accounts and hierarchy maintenance of a parent child relationship of chart of accounts	
2.	Ability to specify a long and short name for each account	
3.	Ability to classify an account as Asset, Liability, Receipt or Charge	
4.	Ability to classify an account based on different control types such as cash accounts, bank accounts, etc. This classification would be useful to filter accounts for different operation such cash receipts and bank receipts	
5.	Ability to maintain sub-ledgers and classify them into different types. E.g. Employee etc.	
6.	Ability to block access to certain accounts code for posting of transaction	
7.	All the transactions should validate the budget allocation amount. If balance budget amount is less than the transaction amount, system should not allow to save the transaction	
8.	Ability to map Profit Centre details to GL Account	
	Accounts Payable	
9.	Ability to make both cash and cheque payments.	
10.	Ability to capture instrument details for cheque payments	
11.	Ability to identify each payment uniquely through a payment voucher	
12.	Ability to interface with Purchasing module to make payments against one or more purchase orders for the same vendor	
13.	Ability to capture the settlement details of vendor's invoice	
14.	Ability to use standard narrations for payment description	
15.	Ability to record a payment using dual entry: debit the charge account and credit the bank/cash account	
16.	Ability to post a payment transaction through a workflow consisting of one or more approvals	
17.	Provide customizable workflow for approval based on payment amount	
18.	Ability to process payments for multiple employees by a single	

S. No.	Functionality	Compliance Code
	voucher (one transaction). E.g. TA and DA	
19.	Ability to process payments in parts. E.g. Advance payments for purchase followed by a settlement payment on a later date.	
20.	Ability to process payments through letter of credit	
21.	While creating the payment voucher, System should validate the Budget allocation.	
22.	Ability to have general payments	
23.	Ability to filtrate the GL accounts related to Advances for the Contingency Advance	
24.	Ability to select one (or) more GL Accounts during bill passing	
	Accounts Receivable	
25.	Ability to capture voucher type of receipt	
26.	Ability for flexibility of various modes of payment: Cheque, Demand Draft etc. in case of Demand Draft, Ability to capture the Bank Code for the DD Drawn bank	
27.	Ability to make receipt for foreign payment; capture foreign currency, amount, exchange rate and equivalent amount in rupees	
28.	Ability to generate a receipt number based on configurable prefix, suffix and running sequence number	
29.	Ability to identify each receipt uniquely	
30.	Ability to use standard narrations for receipt description and provide the edit option to alter it	
31.	Ability to record a receipt using dual entry: credit the receipt account and debit the bank/cash account	
32.	Ability to post a receipt transaction through a workflow consisting of one or more approvals	
33.	Provide customizable workflow for approval based on receipt amount	
34.	Ability to print a receipt voucher and issue the same	
35.	Ability to settle receipts against advance taken	
36.	Ability to have general receipts	
37.	Ability to search the receipt based on the party/receipt number	
38.	Ability to capture the rejected/approved comments for the receipt	
39.	Ability to create deposit challan for the receipts (Cash, Cheques and DDs)	
	Fixed Assets	
40.	Ability to maintain assets as per classification and class of assets	
41.	Ability to recognize purchase requisition separately for assets	

S. No.	Functionality	Compliance Code
42.	• Ability to capture the following information on each asset • Asset code • Description of asset • Date of capitalization • Classification of the asset • Actual cost (including freight, etc.,) • Foreign Currency Cost (if applicable) • Estimated amortization period (in years, in months etc.,) • Method of depreciation • Location of the asset • Supplier • Purchase order details of the asset • Person to whom the FA is assigned, if applicable • Remarks (if any)	
43.	Ability to calculate depreciation automatically as per the defined rates.	
44.	Ability to generate Fixed asset report as per statutory compliance.	
45.	Ability to handle multiple currencies.	
46.	Ability to pass automatic entries for depreciation and disposable of assets	
	Budgeting Process	
	Master	
47.	Ability to maintain multiple budgets	
48.	Ability to provide options to record budgets at different levels: • At group of accounts • At account level	
49.	Ability to maintain different classification of budgets like Income Budget, Expense Budget etc.	
50.	Ability to attach a specific budget to division/department	
51.	Ability to automatically distribute budgets based on predefined formulas :(months, quarter, etc.) based on prior trends	
52.	Can the system allow users to manually update the budget figures based on a month-on-month basis	
	Transactions	
53.	Ability to provide the option to block the budget amount	
54.	Ability to maintain the allocation of budget amount on the monthly basis	
55.	Ability to track the usage of the budget amount	
	Journal Entries	
56.	Maintain journal entries for any type of transaction including adjustments and contra entries (Transfers)	
57.	Ability to customize workflow for approval based on journal	

S. No.	Functionality	Compliance Code
	amount	
58.	Ability to post journal transactions	
59.	Ability to capture instrument details in journal entries	
60.	Ability to maintain the transaction types for journal entries. Ex Contra Entry and Journal Voucher	
61.	Ability to validate the Budget allocation against any charge account transaction	
62.	Ability to cancel a journal entry	
63.	Ability to filtrate the Cash / Bank accounts for journal entries	
	Bank Reconciliation	
64.	Maintain individual bank accounts within the chart of accounts.	
65.	Ability to upload bank statements in electronic format.	
66.	Ability for automatic reconciliation of bank statements. At challan level for Receipts and at Cheque level for Payments.	
67.	Ability for Manual reconciliation of bank statements	
68.	Ability to include bank issued valid cheque numbers and deposit challan numbers.	
69.	Ability to create voucher for bank charges and interest	
70.	Ability to generate report on unmatched transactions	
	Consolidation	
71.	Ability to define financial/accounting periods	
72.	Ability to perform weekly, monthly and yearly consolidations. Yearly consolidation shall include year-end closing procedure with following steps: Calculation of excess of receipts over payments and move this amount into a liability account and re-initiation of receipt and charge accounts to zero for the next financial period	
73.	Ability to prevent further transaction creation for a period (e.g. month) after period-end process has been completed	
	Budget Preparation	
74.	Ability to define different budget periods	
75.	Ability to capture budget manually for all receipt and charge accounts	
76.	Ability to review/approve budget through work flow	
	Integration with other modules	
77.	Ability to interface with Payroll module for automatic posting the pay-slip transactions to finance application. During posting certain accounts may be consolidated	
78.	Ability to interface with HRMS and Payroll modules for disbursement of TA and DA for employee.	
79.	Ability to interface with HRMS and Payroll for automatic creation of voucher	

S. No.	Functionality	Compliance Code
	General	
80.	Ability to Attach Documents while creating transactions.	
81.	Ability to capture Grace Period to make adjustments in the previous period transactions. E.g.: If Grace period is 15 days, then the system should allow the user to make adjustments till 15th April only if the period end date is 31st March	
82.	Ability to allow the employee to access only their respective GL accounts	
83.	Ability to copy all type of transactions for fast data entry	
84.	Ability to process foreign currency details irrespective of the instruments type	
85.	Ability to review/approve/reject/ post all type of transactions	
86.	Ability to filtrate the GL account based on the instrument type	
87.	Ability to cancel the approved transactions	
	Reports	
88.	Ability to generate Cash Ledger report	
89.	Ability to generate Bank Ledger report	
90.	Ability to generate Journal Ledger report with ability to include transactions from past financial periods for certain reports such as utilization reports in plan account.	
91.	Ability to generate Bank Reconciliation Report	
92.	Ability to generate Trial Balance report	
93.	Ability to generate Receipt and Charge Statement, including budget figures	
94.	Ability to generate Receipt and Charge Statement, including budget figures for CPF, Pension Fund	
95.	Ability to generate Balance Sheet	
96.	Ability to generate Balance Sheet for CPF, Pension Fund	
97.	Ability to generate Ledger Report for all GL accounts (Assets, Liabilities, Receipts and Expenses)	
98.	Ability to generate report on Demand Draft Forwarding Register	
99.	Ability to generate report on Yearly Extract on PF received	
100.	Ability to generate Form 16A, 26Q for the TDS deducted	
101.	Ability to generate report on Income and Expenditure Account for CPF, Pension Fund	
102.	Ability to generate report on Chart of accounts	
103.	Ability to generate Statement of tax deduction	
104.	Ability to generate report on Tax deduction	
105.	Ability to generate Certificate of Tax Deduction at Source	
106.	Ability to generate Covering Letter for Bills / Cheque	

S. No.	Functionality	Compliance Code
107.	Ability to generate the Cash Flow report	
108.	Ability to generate the Fund Flow report	
109.	Ability to generate Monthly Sale tax, Income tax Reports	
110.	Ability to generate reports for comparing budgets against actual transactions	

4.17 Electronic Record Management System

The envisaged Electronic Records Management Systems should have the following attributes to ensure that Authenticity, Reliability, Integrity and Usability of records are maintained:

- Creating records in context – electronic records management systems will enable CCI to capture evidence of their business activity. This involves identifying a set of electronic information to serve as the evidential record comprising both content and context.
- Records management metadata will be configurable – to be meaningful as evidence of a business process, records will be linked to the context of their creation and use. To do this, the record will be associated with metadata about the business context in a classification structure. In addition to this 'classification' metadata, other metadata that should be captured at the point of creation includes:
    i. Record identifier (Case Number);
    ii. Date of creation;
    iii. Creator/author/person responsible; and
- The business being conducted etc.
    i. Records can be reassigned or reclassified, closed and if required, duplicated and extracted
    ii. Reports can be generated – on records and the management thereof.
    iii. Security processes– normal systems controls over access and security to support the maintenance of authenticity, reliability, integrity and usability.
    iv. Records will be retained for a period of time that is in accordance with the policies defined by CCI.

The system should be integrated with RFID Tracking Application for record management

4.17.1 Technical Specifications

S. No.	Functionality	Compliance Code
1.	Enable integration with business applications so that transactional records created by those applications can be captured within the electronic records management system.	
2.	Indicate when an individual record is captured within the	

S. No.	Functionality	Compliance Code
	electronic records management system.	
3.	Prevent the alteration of the content of any record by any user or administrator during the process of records capture.	
4.	Prevent the destruction or deletion of any record by any user, including an administrator, with the exceptions of: • Destruction in accordance with a disposition authority • Authorised deletion by an administrator	
5.	Support manual naming of electronic records, and allow this name to be different from the existing file name (including email subject lines used to construct record titles). If the existing filename is taken by default, the electronic records management system must allow this name to be amended at the time of capture.	
6.	Allow an administrator to alter the metadata of a record within the system if required, to allow finalisation/correction of the record profile. Any such action must be captured in a records management metadata.	
7.	Any revision or alteration of the records management/capture metadata must be captured as additional records management metadata.	
8.	Alert a user to any failure to successfully capture a record.	
9.	Be able, where possible and appropriate, to provide a warning if an attempt is made to capture a record that is incomplete or inconsistent in a way which will compromise its future apparent authenticity.	
10.	Capture scanned images of incoming documents.	
	Point Of Capture Metadata	
11.	Support the use of persistent metadata for records	
12.	Acquire metadata elements for each record and persistently link them to the record over time.	
13.	Ensure that the values for metadata elements conform to specified encoding schemes.	
14.	Allow the administrator to pre-define (and re-define) the metadata elements associated with each record, including whether each element is mandatory or optional.	
15.	Allow all metadata for every record to be viewed by users, subject to access rights for individuals or groups of users.	
16.	Automatically capture the date and time of capture of each record as metadata elements linked to each record.	
17.	Support automatic extraction or migration of metadata from: • the software application that created the record; • an operating system or line of business system; • an electronic records management system; and • the file header of each record and its constituent components captured into the system.	

S. No.	Functionality	Compliance Code
18.	Prevent the alteration of metadata captured in Requirement 16, unless authorised by the system administrator.	
19.	Allow entry of additional metadata by users during record capture and/or a later stage of processing by the user.	
20.	Ensure that only authorised users and administrators can change the content of records management metadata elements.	
21.	Allocate an identifier, unique within the system, to each record at point of capture automatically.	
	Aggregation Of Electronic Records	
22.	Ensure that all records captured within the electronic records management system are associated with at least one aggregation.	
23.	Manage the integrity of all markers or other reference tags to records (where used), ensuring that: • following a marker, whichever aggregation that the marker record is located in, will always result in correct retrieval of the record; and • any change in location of a record also redirects any marker that references that record.	
24.	Not impose any practical limit on the number of records that can be captured in an aggregation, or on the number of records that can be stored in the electronic records management system. However, the system may permit the administrator to set limitations on the quantity of items within an aggregation if required for business purposes.	
25.	Allow users to choose at least one of the following where an electronic object has more than one manifestation: • register all manifestations of the object as one record; • register each manifestation of the object as a discrete record.	
26.	Support the ability to assign records to multiple aggregations without their duplication.	
	Bulk Importing	
27.	Be able to capture in bulk records exported from other systems, including capture of: • electronic records in their existing format, without degradation of content or structure, retaining any contextual relationships between the components of any individual record; • electronic records and all associated records management metadata, retaining the correct contextual relationships between individual records and their metadata attributes; and • the structure of aggregations to which the records are assigned, and all associated records management metadata, retaining the correct relationship between records and aggregations	
28.	Be able to import any directly associated event history metadata	

S. No.	Functionality	Compliance Code
	with the record and/or aggregation, retaining this securely within the imported structure.	
	Electronic Document Formats	
29.	Support the capture of records created in native file formats from commonly used software applications such as: • standard office applications (word processing, spread-sheeting, presentation, simple databases); • email client applications; • imaging applications; and • web authoring tools. Not apply any practical limit to record types or format for capture.	
30.	Be able to extend the range of file formats supported as new file formats are introduced for business purposes or for archival retention (for example, PDF/A).	
	Compound Records	
31.	Capture compound electronic records (records comprising more than one component) so that: • the relationship between the constituent components of each compound record is retained; • the structural integrity of each compound record is retained; and • each compound record is retrieved, displayed and managed as a single unit.	
32.	Be able to capture compound records easily, preferably with one action, for example, a single click.	
	Email	
33.	Allow users to capture emails (text and attachments) as single records as well as individual records linked by metadata	
34.	Allow individual users to capture email messages (and attachments) from within their email application.	
35.	Allow users to choose whether to capture emails with attachments as: • email text only; • email text with attachments; or • attachments only.	
36.	Ensure the capture of email transmission data as metadata persistently linked to the email record.	
37.	Ensure that the text of an email and its transmission details cannot be amended in any way once the email has been captured. Nor should the subject line of the email itself be changeable, although the title of the record may be edited for easier access through, for example, keywords or by file-naming conventions.	
38.	Ensure that a human-readable version of an email message	

S. No.	Functionality	Compliance Code
	address is also captured, where one exists.	
	Identification	
39.	Associate each of the following with a unique identifier: • record; • record extract; and • aggregation	
40.	Require all identifiers to be unique and unduplicated within the entire electronic records management system.	
41.	Be able to store the unique identifiers as metadata elements of the entities to which they refer	
42.	Generate unique identifiers automatically, and prevent users from inputting the unique identifier manually and from subsequently modifying it (for example, a sequential number)	
43.	Allow the format of the unique identifier to be specified at configuration time. Where unique identifiers are automatically generated, the electronic records management system should:	
44.	Allow the administrator to specify at configuration time the starting number (for example, 1, 10, 100) and increment (for example, 1, 10) to be used in all cases.	
	Classification	
45.	Support and be compatible with the organisational classification scheme.	
46.	Be able to support a classification scheme that can represent aggregations (at the function, activity, transaction level) as being organised in a hierarchy with a minimum of five levels.	
47.	Allow the inheritance of values from a classification scheme.	
48.	Allow naming conventions or thesauri to be defined at the time the electronic records management system is configured.	
49.	Support the initial and on-going construction of a classification scheme.	
50.	Allow administrators to create new aggregations at any level within any existing aggregation.	
51.	Not limit the number of levels in the classification scheme hierarchy unless set by an administrator.	
52.	Support the definition of different record types that are associated with a specified set of metadata to be applied at capture.	
53.	Support the allocation of unique identifiers to records within the classification structure	
54.	Where the unique identifiers are based on sequential numbering, the electronic records management system should: Have the capacity to automatically generate the next sequential number within the classification scheme for each new electronic aggregation.	

S. No.	Functionality	Compliance Code
55.	May support a distributed classification scheme that can be maintained across a network of electronic record repositories	
56.	Where the electronic records management system employs a graphical user interface, it must: Support browsing and graphical navigation of the aggregations and classification scheme structure, and the selection, retrieval and display of electronic aggregations and their contents through this mechanism.	
57.	Should support the definition and simultaneous use of multiple classification schemes This may be required, for example, following the merger of two organisations or migration of legacy systems. It is not intended for routine use.	
	Classification Levels	
58.	Support metadata for levels within the classification scheme.	
59.	Provide at least two naming mechanisms for records in the classification scheme: • a mechanism for allocating a structured alpha, numeric or alphanumeric reference code (that is, an identifier which is unique within the classification scheme) to each classification level; and • a mechanism to allocate a textual title for each electronic aggregation. It must be possible to apply both identifiers separately or together.	
60.	Allow only authorised users to create new classifications at the highest level in the classification scheme (for example, at the business function level).	
61.	Automatically include in the records management metadata of each new aggregation those attributes that derive from its position in the classification scheme (for example, name, and classification code).	
62.	Allow the automatic creation and maintenance of a list of classification levels	
63.	Support a naming mechanism that is based on controlled vocabulary terms and relationships drawn (where appropriate) from an ISO 2788-compliant or ISO 5964-compliant thesaurus and support the linking of the thesaurus to the classification scheme	
64.	Support an optional aggregation naming mechanism that includes names (for example, people's names) and/or dates (for example, dates of birth) as file names, including validation of the names against a list	
65.	Support the allocation of controlled vocabulary terms compliant with ISO 2788 or ISO 5964 as records management metadata, in addition to the other requirements in this section	

S. No.	Functionality	Compliance Code
	Classification Processes	
66.	Allow an electronic aggregation (including volumes) to be relocated to a different position in the classification scheme, and ensure that all electronic records already allocated remain allocated to the aggregations (including volumes) being relocated.	
67.	Allow an electronic record to be reclassified to a different volume of an electronic aggregation.	
68.	Restrict to Administrators and Records Manager the ability to move aggregations (including volumes) and individual records.	
69.	Keep a clear history of the location of reclassified aggregations (including volumes) prior to their reclassification, so that their entire history can be determined easily.	
70.	Prevent the deletion of an electronic aggregation or any part of its contents at all times, with the exceptions of: • destruction in accordance with a disposal authority; and • deletion by an administrator as part of an audited procedure.	
71.	Allow an electronic aggregation to be closed by a specific administrator procedure, and restrict this function to an administrator.	
72.	Record the date of closing of a volume in the volume's records management metadata.	
73.	Maintain internal integrity (relational integrity or otherwise) at all times, regardless of: • maintenance activities; • other user actions; and • failure of system components.	
74.	Not allow any volume that has been temporarily re-opened to remain open after the administrator who opened it has logged off.	
75.	Allow users to create cross-references between related aggregations or between aggregations and individual records.	
76.	Provide reporting tools for the provision of statistics to the administrator on aspects of activity using the classification scheme, including the numbers of electronic aggregations (including volumes) or records created, closed or deleted within a given period, by user group or functional role.	
77.	Allow the Administrators and Records Manager to enter the reason for the reclassification of aggregations (including volumes) and individual records.	
78.	Be able to close a volume of an electronic aggregation automatically on fulfilment of specified criteria to be defined at configuration, including at least: • volumes delineated by an annual cut-off date (for example, end	

S. No.	Functionality	Compliance Code
	of the calendar year, financial year or other defined annual cycle); • the passage of time since a specified event (for example, the most recent addition of an electronic record to that volume); and • the number of electronic records within a volume.	
79.	Be able to open a new volume of an electronic aggregation automatically on fulfilment of specified criteria to be defined at configuration	
80.	Allow an administrator to lock or freeze aggregations to prevent relocation, deletion, closure or modification when circumstances require, for example, pending legal action	
	Record Volumes	
81.	Allow administrators to add (open) electronic volumes to any electronic aggregation that is not closed.	
82.	Record the date of opening of a new volume in the volume's records management metadata.	
83.	Automatically include in the metadata of new volumes those attributes of its parent aggregation's records management metadata that assign context (for example, name, and classification code).	
84.	Support the concept of open and closed volumes for electronic aggregations, as follows: • only the most recently created volume within an aggregation can be open; and • all other volumes within that aggregation must be closed	
85.	Prevent the user from adding electronic records to a closed volume	
	Access And Security	
86.	Ensure that records are maintained complete and unaltered	
87.	Maintain the technical, structural and relational integrity of records and metadata in the system.	
	Access Controls	
88.	Restrict access to system functions according to a user's role and strict system administration controls	
	Establishing Security Control	
89.	Allow only administrators to set up user profiles and allocate users to groups.	
90.	Allow the administrator and Records Manager to limit access to records, aggregations and records management metadata to specified users or user groups.	
91.	Allow the administrator and Records Manager to alter the security category of individual records.	
92.	Allow changes to security attributes for groups or users (such as access rights, security level, privileges, initial password allocation	

S. No.	Functionality	Compliance Code
	and management) to be made only by the administrator.	
	Assigning Security Levels	
93.	Allow only the administrator and Records Manager to attach to the user profile attributes that determine the features, records management metadata fields, records or aggregations to which the user has access. The attributes of the profile will: • prohibit access to the electronic records management system without an accepted authentication mechanism attributed to the user profile; • restrict user access to specific records or aggregations; • restrict user access according to the user's security clearance; • restrict user access to particular features (for example, read, update and/or delete specific records management metadata fields); • deny access after a specified date; and • allocate the user to a group or groups.	
94.	Be able to provide the same control functions for roles, as for users.	
95.	Be able to set up groups of users that are associated with an aggregation.	
96.	Allow a user to be a member of more than one group.	
97.	Be able to limit users' access to parts of the list (to be specified at the time of configuration).	
	Executing Security Controls	
98.	Allow the administrator and Records Manager, to alter the security category of all records within an aggregation in one operation. The electronic records management system must provide a warning if the security classifications of any records are lowered, and await confirmation before completing the operation	
99.	Allow the administrator and Records Manager to change the security category of aggregations, subject to the requirements of Section 3.4.6: Security Categories.	
100.	Record full details of any change to security category in the records management metadata of the record, volume or aggregation affected.	
101.	Provide one of the following responses (selectable at configuration time) whenever a user requests access to, or searches for, a record, volume or aggregation that they do not have the right to access: • not display any record information or indicate its existence in any way.	
102.	Never include, in a list of full text or other search results, any record that the user does not have the right to access.	
103.	Log all unauthorised attempts to access aggregations (and their volumes) or records in their respective unique metadata.	

S. No.	Functionality	Compliance Code
	Security Categories	
104.	Allow security classifications to be assigned to records.	
105.	Allow security classifications to be selected and assigned at system level for: • all levels of records aggregations (including volumes); and • individual records or record objects.	
106.	Allow access-permission security categorisation to be assigned: • at group level (be able to set up group access to specific aggregations, record classes security or clearance levels); • by organisational role; • at user level; and in combination(s) of the above	
107.	Allow the assignment of a security category: • at any level of records aggregation; • after a specified time or event; and • to a record type.	
108.	Support the automated application of a default value of 'Unclassified' to an aggregation or record not allocated any other security category.	
109.	Enable its security subsystem to work effectively together with general security products.	
110.	Be able to determine the highest security category of any record in any aggregation by means of one simple enquiry.	
111.	Support routine, scheduled reviews of security classifications.	
112.	Restrict access to electronic aggregations/records that have a security classification higher than a user's security clearance.	
113.	Be capable of preventing an electronic aggregation from having a lower security classification than any electronic record within that aggregation.	
	Records Management Process Metadata	
114.	Be capable of creating unalterable metadata of records management actions (actions to be specified by the client) that are taken on records, aggregations or the classification scheme. The metadata should include the following records management metadata elements: • type of records management action; • user initiating and/or carrying out the action; and date and time of the action	
115.	Track events without manual intervention and store information in the metadata once the metadata functionality has been activated.	
116.	Maintain the metadata for as long as required.	
117.	Provide metadata of all changes made to: • electronic aggregations (including volumes); • individual electronic records; and • records management metadata associated with any of the	

S. No.	Functionality	Compliance Code
	above.	
118.	Document all changes made to administrative parameters (for example, changes made by the administrator to a user's access rights).	
119.	Be capable of capturing and storing in the metadata information about the following actions: • date and time of capture of all electronic records; • reclassification of an electronic record in another electronic volume; • reclassification of an electronic aggregation in the classification scheme; • any change to the disposal authority of an electronic aggregation; • any change made to any records management metadata associated with aggregations or electronic records; • date and time of creation, amendment and deletion of records management metadata; • changes made to the access privileges affecting an electronic aggregation, electronic record or user; • export or transfer actions carried out on an electronic aggregation; • date and time at which a record is rendered; and • disposal actions on an electronic aggregation or record.	
120.	Be able to export metadata for specified records and selected groups of records without affecting the metadata stored by the electronic records management system.	
121.	Be able to capture and store violations (that is, a user's attempts to access a record or aggregation, including volumes, to which they are denied access), and (where violations can validly be attempted) attempted violations of access control mechanisms.	
122.	Be able, at a minimum, to provide reports for actions on records and aggregations organised: • by record or aggregation; • by file listing (list of entire files in e-file plan/classification scheme) • by file listing and description • by user; and	
123.	Allow the metadata facility to be configurable by the administrator so that the functions for which information is automatically stored can be selected. The electronic records management system must ensure that this selection and all changes to it are stored in the metadata	
124.	Be able to provide reports for actions on aggregations and records organized by workstation and (where technically appropriate) by network address.	
125.	Allow the administrator to change any user-entered records	

S. No.	Functionality	Compliance Code
	management metadata element. Information about any such change must be stored in the metadata.	
	Tracking Records Movement	
126.	Provide a tracking feature to monitor and record information about the location and movement of both electronic and non-electronic aggregations.	
127.	Record information about movements including: • unique identifier of the aggregation or record; • current location as well as a user-defined number of previous locations (locations should be user-defined); • date item sent/moved from location; • date item received at location (for transfers); and • user responsible for the move (where appropriate).	
128.	Maintain access to the electronic record content, including the ability to render it, and maintenance of its structure and formatting over time and through generations of office application software.	
	Hybrid Records Management: Management of Electronic And Non-Electronic Records	
129.	Be able to define in the classification scheme non-electronic aggregations and volumes, and must allow the presence of non-electronic records in these volumes to be reflected and managed in the same way as electronic records.	
130.	Allow both kinds of records to be managed in an integrated manner.	
131.	Allow a non-electronic aggregation that is associated as a hybrid with an electronic aggregation to use the same title and numerical reference code, but with an added indication that it is a hybrid non-electronic aggregation.	
132.	Allow a different records management metadata element set to be configured for non-electronic and electronic aggregations; non-electronic aggregation records management metadata must include information on the physical location of the non-electronic aggregation.	
133.	Ensure that retrieval of non-electronic aggregations displays the records management metadata for both electronic and non-electronic records associated with it.	
134.	Include features to control and record access to non-electronic aggregations, including controls based on security category, which are comparable with the features for electronic aggregations.	
135.	Support tracking of non-electronic aggregations by the provision of request, check-out and check-in facilities that reflect the current location of the item concerned.	
136.	Support the printing and recognition of bar codes for non-	

S. No.	Functionality	Compliance Code
	electronic objects (for example, documents, files and other containers), or should support other tracking systems to automate the data entry for tracking the movement of such non-electronic records.	
137.	Support the retention and disposal protocols and routinely apply to both electronic and non-electronic elements within hybrid aggregations. Where aggregations have security categories, the electronic records management system must:	
138.	Ensure that a non-electronic record is allocated the same security category as an associated electronic record within a hybrid records aggregation.	
	Retention And Disposal: Records Disposal Schedule	
139.	Provide a function that: • specify disposal authorities; • automates reporting and destruction actions; • disposes of compound records as a single action; and • provides integrated facilities for exporting records and records management metadata.	
140.	Be able to restrict the setting up and changing of records disposal schedule to the administrator and Records Manager.	
141.	Allow the administrator to define and store a set of customised standard records disposal schedule.	
142.	Be capable of assigning a records disposal schedule to any aggregation or record type.	
143.	By default, ensure that every record in an aggregation is governed by the records disposal schedule associated with that aggregation.	
144.	Include a disposition action, agency retention period and trigger in the (metadata) record for the decision for each records disposal schedule.	
145.	For each aggregation: • automatically track retention periods that have been allocated to the aggregation; and • initiate the disposition process by prompting the administrator to consider and, where appropriate approve and execute, disposal action when disposition is due.	
146.	Allow at least the following decisions for each records disposal schedule: • retain indefinitely; • present for review after a specified date or timeframe; • destroy after a specified date or timeframe; and • transfer after a specified date or timeframe.	
147.	Allow retention periods for each records disposal schedule to be specified with the date which is able to be set in at least the	

S. No.	Functionality	Compliance Code
	following ways: • Date Created; • Date Closed; • Date Registered; • Last Action Date; • Date Modified; • Date Archived; • User Defined;	
148.	Enable a retention period to be assigned to an aggregation that over-rides the retention period assigned to its 'parent' aggregation.	
149.	Allow the administrator to amend any retention period allocated to any aggregation at any point in the life of that aggregation.	
150.	Allow the administrator to change the retention period associated with an aggregation at any time.	
151.	Allow the definition of sets of processing rules that can be applied as an alerting facility to specified aggregations prior to initiation of a disposal process.	
152.	Provide the option of allowing electronic records or aggregations that are being moved between aggregations by the administrator or records manager to have the retention period of the new aggregation, replacing the existing retention period applying to these records.	
	Executing records disposal schedules	
153.	Allow the administrator to delete aggregations, volumes and records upon maturity of their retention periods as specified in the records disposal schedules	
154.	When executing records disposal schedules, the electronic records management system must be able to: • produce an exception report for the administrator; • delete the entire contents of an aggregation or volume including backup copies when it is deleted to ensure the deletion is irreversible and the information cannot be recovered or reconstructed; • prompt the administrator to enter a reason for the action; • alert the administrators to any conflicts, for example, items that are linked to more than one disposition action involving pointers; and • maintain complete integrity of the records management metadata at all times. Automatically track all retention periods specified in these records disposal schedules, and initiate the disposal process once the last of all these retention dates is reached.	
155.	Allow the administrator to manually or automatically lock or freeze records disposition processes (freeze for litigation or legal	

S. No.	Functionality	Compliance Code
	discovery purposes, Freedom of Information purposes, etc.).	
	Documenting disposition actions	
156.	Record any deletion or disposal action comprehensively in the process metadata.	
157.	Automatically record and report all disposal actions to the administrator.	
	Reviewing disposition	
158.	Support the review process by presenting electronic aggregations to be reviewed, with their records management metadata and information on retention periods, in a manner that allows the reviewer to browse the contents of the aggregation and/or records management metadata efficiently.	
159.	Allow the reviewer to take at least any one of the following actions for each aggregation during review: • mark the aggregation for destruction; • mark the aggregation for transfer; • mark the aggregation for indefinite hold, for example, pending litigation; and • change the disposal authority (or assign a different schedule) so that the aggregation is retained and re-reviewed at a later date, as defined in this section.	
160.	Allow the reviewer to enter comments into the aggregation's records management metadata to record the reasons for the review decisions.	
161.	Alert the administrator to aggregations due for disposal before implementing disposal actions, and seek confirmation from the administrator before initiating the disposal actions.	
162.	Always seek confirmation of disposal actions twice before proceeding.	
163.	Store in the metadata all decisions taken by the reviewer during reviews.	
164.	Produce a records disposal schedules report for the administrator that identifies all retention periods that are due to be applied in a specified time period, and provide quantitative reports on the quantity and types of records covered.	
165.	Be able to specify the frequency of a records disposal schedules report, the information reported and highlight exceptions such as overdue disposal.	
166.	Alert the administrator if an electronic aggregation that is due for destruction is referred to in a link from another aggregation and pause the destruction process to allow the following remedial action to be taken: • confirmation by the administrator to proceed with or cancel the process; and	

S. No.	Functionality	Compliance Code
	• generation of a report detailing the aggregation or record(s) concerned and all references or links for which it is a destination.	
167.	Support reporting and analysis tools for the management of records disposal schedules by the administrator, including the ability to: • list all retention periods; • list all electronic aggregations to which a specified records disposal schedule/retention period is assigned; • list the retention periods applied to all aggregations below a specified point in the hierarchy of the classification scheme; • identify, compare and review retention periods (including their contents) across the classification scheme; and • identify formal contradictions in retention periods across the classification scheme.	
168.	Provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process by tracking: • progress/status of the review, such as awaiting or in-progress, details of reviewer and date; • records awaiting disposal as a result of a review decision; and • progress of the transfer process.	
169.	Be able to accumulate statistics of review decisions in a given period and provide tabular and graphic reports on the activity.	
	Migration And Export	
170.	Provide a well-managed process to transfer records to another system or to a third party organisation and support migration processes.	
171.	Include all aggregations, volumes, records and associated metadata within aggregations whenever an electronic records management system transfers any aggregation or volume.	
172.	Be able to transfer or export an aggregation (at any level) in one sequence of operations so that: • the content and structure of its electronic records are not degraded; • all components of an electronic record (when the record consists of more than one component) are exported as an integral unit including any technical protection measures; • all links between the record and its records management metadata are retained; and • all links between electronic records, volumes and aggregations are retained.	
173.	Be able to include a copy of the entire metadata set associated with the records and aggregations that are transferred or exported from an electronic records management system.	
174.	Provide a utility or conversion tool to convert the entire metadata	

S. No.	Functionality	Compliance Code
	set associated with the records and aggregations that are transferred or exported into XML format	
175.	Produce a report detailing any failure during a transfer, export or destruction. The report must identify any records destined for transfer that have generated processing error, and any aggregations or records that are not successfully transferred, exported or destroyed.	
176.	Retain copies of all electronic aggregations and their records that have been transferred to archives, at least until such time as a successful transfer is confirmed. Any deletion before confirmation of a successful transfer is prohibited	
177.	Have the ability to retain records management metadata for records and aggregations that have been destroyed or transferred.	
178.	Be able to export records in their native format or current format to which they have been migrated and in order of reference.	
179.	Be able to export all types of records which it is able to capture	
180.	Provide the ability to add user-defined records management metadata elements required for archival management purposes to electronic aggregations selected for transfer.	
181.	Provide the ability to sort electronic aggregations selected for transfer into ordered lists according to user-selected records management metadata elements.	
182.	Require the administrator to confirm that the non-electronic part of the same aggregations has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part.	
	Retention And Disposal Of Electronic And Non-Electronic Records	
183.	Support the allocation of records disposal schedule to every non-electronic aggregation in the classification scheme. The records disposal schedule must function consistently for electronic and non-electronic aggregations, notifying the administrator when the disposal date is reached, but taking account of the different processes for disposing of electronic and non-electronic records.	
184.	Support the application of the same records disposal schedule to both the electronic and non-electronic aggregations that make up a hybrid aggregation.	
185.	Be able to apply any review decision made on a hybrid electronic aggregation to a non-electronic aggregation with which it is associated.	
186.	Alert the administrator to the existence and location of any hybrid non- electronic aggregation associated with a hybrid electronic aggregation that is to be exported or transferred.	

S. No.	Functionality	Compliance Code
187.	Be able to record in the metadata all changes made to records management metadata references to non-electronic or hybrid aggregations and records.	
188.	Be capable of offering check-out and check-in facilities for non-electronic aggregations profiled in the system, in particular enabling the ability to record a specific user or location to which a non-electronic aggregation is checked out, and to display this information if the non-electronic aggregation is requested by another user.	
189.	Be capable of offering a request facility for non-electronic records profiled in the hybrid aggregation system, enabling a user to enter a date that the non- electronic element is required and generating a consequent message for transmission to the current holder of that non-electronic aggregation or the administrator, according to configuration.	
190.	Be able to export and transfer records management metadata of non- electronic records and aggregations.	
191.	Support the application of a review decision taken on a group of aggregations to any non-electronic aggregations within that group, by notifying the administrator of necessary actions to be taken on the non-electronic aggregations.	
	Disseminate: Search, Retrieve And Render (Display)	
192.	Provide a flexible range of functions that operate on the metadata related to every level of aggregation and on the contents of the records through user- defined parameters for the purpose of locating, accessing and retrieving individual records or groups of records and/or metadata.	
193.	Allow all record, volume and aggregation records management metadata to be searchable.	
194.	Allow the text contents of records (where they exist) to be searchable.	
195.	Allow the user to set up a single search request with combinations of records management metadata and/or record content.	
196.	Allow administrators to configure and change the search fields to: • specify any element of record, volume and aggregation records management metadata, and optionally full record content, as search fields; and • change the search field configuration.	
197.	Provide searching tools for: • Free-text searching of combinations of record and aggregation records management metadata elements and record content; and • Boolean searching of records management metadata elements	
198.	Provide for ‘wild card’ searching of records management	

S. No.	Functionality	Compliance Code
	metadata that allows for forward, backward and embedded expansion.	
199.	Allow searching within a single aggregation or across more than one aggregation.	
200.	Be able to search for, retrieve and display all the records and records management metadata relating to an electronic aggregation, or volume, as a single unit.	
201.	Be able to search for, retrieve and render an electronic aggregation by all implemented naming principles, including: • name; and • identifier (classification code).	
202.	Display the total number of search results on a user's screen and must allow the user to then display the results list, or refine the search criteria and issue another request.	
203.	Allow records and aggregations featured in the search results list to be selected, then opened (subject to access controls) by a single click or keystroke.	
204.	Allow users to retrieve aggregations and records directly through the use of a unique identifier.	
205.	Never allow a search or retrieval function to reveal to a user any information (records management metadata or record content) that the access and security settings are intended to hide from that user.	
206.	Have integrated search facilities for all levels of the classification scheme.	
207.	Provide free-text and records management metadata searches in an integrated and consistent manner.	
208.	Present seamless functionality when searching across electronic, non-electronic and hybrid aggregations.	
209.	Allow users to save and re-use queries.	
210.	Allow users who are viewing or working with a record or aggregation, whether as the result of a search or otherwise, to see the record within the classification or aggregation hierarchy easily and without leaving or closing the record.	
211.	Allow users to refine (that is, narrow) searches.	
212.	Provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a search result	
213.	Allow the records management metadata of any object (such as record, volume or aggregation) to be searched, whether the object itself is in electronic form or not, and regardless of whether the object is stored online, near-line or offline.	
214.	Provide display formats configurable by users or administrators for search results, including such features and functions as: • select the order in which the search results are presented;	

S. No.	Functionality	Compliance Code
	• specify the number of search results displayed on the screen; • set the maximum number of search results; • save the search results; and • choose which records management metadata fields are displayed in search result lists.	
215.	Provide a browsing mechanism that enables graphical or other display browsing techniques at any level of aggregation.	
	Rendering: Displaying Records	
216.	Render or download records that the search request has retrieved.	
217.	Render records that the search request has retrieved without loading the associated application software. The document viewer should be capable of displaying all the file formats in use in CCI	
218.	Be able to render all the types of electronic records specified by the organisation in a manner that preserves the information in the records (for example, all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record in their original relationship.	
	Rendering: Printing	
219.	Provide the user with flexible options for printing records and their relevant records management metadata, including the ability to print a record(s) with records management metadata specified by the user.	
220.	Allow the printing of records management metadata for an aggregation.	
221.	Allow the user to be able to print out a summary list of selected records (for example, the contents of an aggregation), consisting of a user-specified subset of records management metadata elements (for example, Title, Author, Creation date) for each record.	
222.	Allow the user to print the results list from all searches.	
223.	Be able to print all the types of electronic records currently created by the public offices in Malaysia. Printing must preserve the layout produced by the generating application package(s) and include all (printable) components of the electronic record.	
224.	Allow the administrator to specify that all printouts of records have selected records management metadata elements appended to them, for example, title, registration number, and date and security category.	
225.	Allow the administrator to print the thesaurus, where a thesaurus exists within the system.	
226.	Allow the administrator to print any and all administrative parameters.	
227.	Allow the administrator to print records disposal schedules.	

S. No.	Functionality	Compliance Code
228.	Allow the administrator to print the classification scheme.	
229.	Allow the administrator to print metadata schema or element sets	
230.	Allow all records in an aggregation to be printed, in the sequence specified by the user, in one operation.	
231.	Allow the administrator to print the file list.	
	Rendering: Redacting Records	
232.	Allow the administrator to take a copy of a record for the purposes of redaction.	
233.	Record the creation of extracts in the records management metadata, including at least date, time, reason for creation and creator.	
234.	Store in the metadata any change made in response to the requirements in this section.	
235.	Provide functionality for redacting sensitive information from the extract. If the electronic records management system does not directly provide these facilities, it must allow for other software packages to do so.	
236.	Prompt the creator of an extract to assign it to an aggregation.	
237.	Store a cross-reference to an extract in the system.	
	Rendering: Other	
238.	Include features for rendering those records that cannot be meaningfully printed to an appropriate output device.	
	Rendering: Re-Purposing Content	
239.	Allow the re-use or re-purposing of content.	
	Administrator functions	
240.	Allow the administrator to retrieve, display and re-configure system parameters and to re-allocate users and functions between user roles.	
241.	Provide back-up facilities so that records and their records management metadata can be recreated using a combination of restored back-ups and metadata.	
242.	Provide recovery and rollback facilities in the case of system failure or update error, and must notify the administrator of the results.	
243.	Monitor available storage space and notify the administrator when action is needed because available space is at a low level or because it needs other administrative attention.	
244.	Allow the administrator to make bulk changes to the classification scheme, ensuring all records management metadata and metadata data are handled correctly and completely at all times, in order to make the following kinds of organisational change: • division of an organisational unit into two; • movement or re-naming of an organisational unit; and • division of a whole organisation into two organisations.	

S. No.	Functionality	Compliance Code
245.	Support the movement of users between organisational units.	
246.	Allow the definition of user roles, and must allow several users to be associated with each role.	
247.	Communicate errors encountered in storing data	
	Metadata Administration	
248.	Allow the administrator to create, define and delete metadata elements, including custom fields.	
249.	Allow the administrator to apply and modify metadata schema rules, including semantic and syntactical rules, encoding schemes and obligation status.	
250.	Allow the administrator to configure the system to restrict the viewing or modifying of metadata elements by group, functional role or user	
251.	Document all metadata administration activities.	
	Reporting	
252.	Provide flexible reporting facilities for the administrator. They must include, at a minimum, the ability to report the following: • numbers of aggregations, volumes and records; • transaction statistics for aggregations, volumes and records; and • activity reports for individual users.	
253.	Allow the administrator to report on metadata based on selected: • aggregations; • volumes; • record objects; • users; • file formats and instances of each format.	
254.	Be able to produce a report listing aggregations, structured to reflect the classification scheme, for all or part of the classification scheme.	
255.	Allow the administrator to request regular periodic reports and one-off reports.	
256.	Allow the administrator to report on metadata based on selected: • security categories; • user groups; and • other records management metadata.	
	Back-Up And Recovery	
257.	Provide automated back-up and recovery procedures.	
258.	Allow the administrator to schedule back-up routines by: • specifying the frequency of back-up; and • allocating storage media, system or location for the back-up (for example, offline storage, separate system, remote site).	
259.	Allow only the administrator to restore from electronic records management system back-ups. Full integrity of the data must be maintained after restoration.	

S. No.	Functionality	Compliance Code
260.	Allow only the administrator to roll-forward the electronic records management system from a back-up to a more recent state, maintaining full integrity of the data.	
261.	Allow users to indicate that selected records are considered to be 'vital records'.	
262.	Be able to notify users whose updates may have been incompletely recovered, when they next use the system, that a potentially incomplete recovery has been executed.	
	Multimedia Repository	
263.	Allow Asset Management and allow multiple users to edit content and make changes	
264.	Have Editing Tools such as text based editor with spell-check capabilities; ability to consolidate changes from multiple editors; ability to edit within the system as well as external to the system (i.e., in MS Word). If editing is to be done within original application, the application should be integrated with the CMS.	
265.	Allow Multiple Content Sources: Text; Graphic; Database; Multimedia or other.	
266.	Have Creation Templates as well as the ability to use standard and customized templates for content creation within system.	
267.	Have Publishing Templates with standard templates for presentation of material available, as well as ability to customize.	
268.	Have Word Templates and accommodate storage, display of MS Word or other Templates.	
269.	Enable Content Creation such as ability to generate PDF format as needed.	
270.	Have Check-in/Check-out Feature with the ability to check content/document out for editing, ability to track who has documents checked out and block editing of same document already in edit mode.	
271.	Enable separation of Content and Presentation such as the ability to separate the creation and presentation of content through use of templates.	
272.	Enable Content Reuse - ability to reuse content in multiple templates/documents	
273.	Have Collaboration System Features - allow users to work together on content/document	
274.	Enable comments to be attached to specific text - ability to attach comments during the editing process to specific areas of text as well as to the document as a whole.	
275.	Enable archiving of content.	
276.	Allow Version Control - application of version control by content creator, save past versions in system so that can roll back if necessary, track date and time of changes and ability to keep	

S. No.	Functionality	Compliance Code
	comment log.	
277.	Enable tracking of changes between versions and ability to identify and compare changes between document versions.	
278.	Allow self-service authoring for non-technical content providers: Content authors should be able to quickly create materials using standard desktop applications.	
	Workflow	
279.	Have integration-messaging - integration of other channels of communication into workflow, i.e., emails notifications.	
280.	Have workflow process - ability to define multiple steps involving various content types, cross-departmental staff and required actions, include triggers by date (automatic notification to update or archive content) and by actions (creation, deletion, editing, etc.)	
281.	Allow parallel and sequential workflow - ability to allow multiple users to edit content at the same time, and also provide a sequential based workflow.	
282.	Allow workflow queues - with ability to show what content is in what state for a particular user id and what content is in what state for groups of users.	
283.	Allow comments – ability to attach comments to a workflow stage.	
	Metadata and Search	
284.	Enable metadata management - must have a native or integrated metadata management tool, ability to change and add metadata fields, conduct global search and replace content for metadata fields and have ability to export metadata lists.	
285.	Permit thesaurus support – accommodate use of predetermined thesaurus/controlled vocabulary during search.	
286.	Enable cross-references - system must support a cross-reference or synonym function to relate terms from thesaurus.	
287.	Provide drill down interface based on hierarchy.	
288.	Allow limited search - ability to limit scope of search functions to selected topics from hierarchy (combines drill down and search functionality).	
289.	Allow fuzzy searching - ability to recognize misspellings and to suggest alternatives	
290.	Allow attribute searching - ability to search metadata as well as provide text word searching (therefore metadata must be stored in such a way as to accommodate search engine access).	
291.	Allow Administrator to control taxonomy (Designed hierarchy of topics and thesaurus controlled by the administrator and not changeable by users).	
292.	Support Taxonomy (multiple hierarchies for documents) - topics maybe repeated within hierarchy and documents may be linked	

S. No.	Functionality	Compliance Code
	to multiple locations.	
293.	Provide access to external information sources – with ability to provide links to external websites and print content that has listing within the system, i.e., through a catalogue.	
294.	Have ability to relate documents within system.	
	User Interface	
295.	GUI Administration features: All configurations, setup, scheduling and other admin functions accessible through a GUI.	
296.	Customizable interface: Ability to customize the user interface as needed.	
297.	Personalization: Personalize according to user group roles, i.e., internal searcher, external searcher, editors	
298.	Be Browser based - use web based interface for user access to system.	
	Reporting & Administration	
299.	Have reporting tools - include performance, workflow, log file analysis; session analysis and ability to create custom reports as needed.	
300.	Have audit trail - provide audit trails for system activity, including workflow and revision history.	
301.	Provide content caching to provide better response time.	
302.	Provide automatic link checking and validation for internal and external links.	
	Security	
303.	Have role based security - provide security according to user role (Combine with document level security to accommodate different editing/author teams).	
304.	Have document level security - allow security to the document level.	
305.	Allow integrated authentication - provide a user authentication mechanism. (Active Directory/LDAP integration preferred).	
306.	Have compatibility with security technology, for example SSL.	
	Enterprise Content Management	
307.	Have a general release date for all software modules of the proposed CMS solution prior to the date of the supplier proposal.	
308.	Prompt for document metadata - The system shall prompt the user for document metadata at the time of creating, saving or closing a document and at the time of sending an e-mail.	
	Architecture	
309.	Support a three-tiered architecture - the logical and physical separation of metadata storage from document repository storage, and the separation of client processes, server processes and interfacing processes.	
310.	Support the creation of multiple, distributed repositories and	

S. No.	Functionality	Compliance Code
	transparent access to multiple, distributed document repositories from any client.	
311.	Have highly integrated product architecture with tightly integrated back-end application server.	
312.	Be scalable to the number of users, retrieval volume and document storage (provide method of sizing used in determining the CMS platform).	
313.	Support access to repositories and workflow functionality over the Internet and intranet (WAN and LAN).	
314.	Support fail-over back-up and recovery capabilities.	
315.	Support various data storage platforms. Please name.	
316.	Support RDBMS. Please name.	
	Desktop Client	
317.	Support access to the document repositories and workflow functionality through Internet Explorer, Netscape Navigator and other industry-standard browsers.	
	Security / Access	
318.	Support very granular access and security restrictions, including the creation of groups of users with specific document manipulation rights (add documents, delete, view, print, etc.) to designated types of documents (index field) groups of documents (index field) and specific individual documents.	
319.	Be configurable at the case file (collection of documents) and document (multiple pages) levels.	
320.	Permit the security/access restrictions on documents and groups to be modified, and to add/delete members to/from a group.	
321.	Be configurable for a single individual, multiple specific users, all users and other membership parameters.	
322.	Allow a user to belong to more than one group for purposes of document access and hide from view the existence of any documents the current user is not permitted access to.	
	Image Capture	
323.	Support appropriate scanners for the page volumes, but the scanners must be capable of scanning a minimum of 25 ppm.	
324.	Support the following file formats/compression formats: TIFF multi-page files G3 and G4 compression, JPEG, GIF, XML, PDF, WAV, MP3, MPEG, and AVI.	
325.	Support the deletion and re-scanning of pages/documents before committing to disk.	
326.	Support various image enhancement and clean-up techniques such as de- skew, de-speckle and darkening/lightening.	
327.	Support image capture at different dpi.	
328.	Support bi-tonal and gravy-scale image scanning and if possible colour scanning too.	

S. No.	Functionality	Compliance Code
329.	Support imaging of 8-1/2" x 11", legal size, single-sided or double-sided pages (duplex on demand).	
	Image Capture Indexing	
330.	Support automatic indexing through barcode recognition for interleaved 3 of 9.	
	Document Management	
331.	Support a hierarchical organization of documents in folders (files).	
332.	Support multiple formats of documents in a single folder.	
333.	Be able to produce an audit trail for various document activities such as add, delete, view, print, etc.	
334.	Support concurrent read/print access to documents by multiple users.	
335.	Provide the capability to restrict document manipulation functions (add, delete, modify) to certain users based on user-selectable parameters (e.g., case type and document type).	
336.	Support digitally signed objects.	
337.	Have the capability to rendition documents from MS Word to PDF format or others. Please name.	
338.	Provide the capability to any user to view or "play" any electronic object types stored in the repository.	
339.	Provide convenient page viewing features such as rotate, zoom, go to "n" page; book marks, etc.	
340.	Support XML documents or other formats. Please name.	
341.	Provide creation, viewing and printing of annotations on documents, pages and folders.	
342.	NOT store annotations in image headers.	
343.	Be able to catalogue documents that are stored off-line.	
344.	Restrict access to annotations to authorized users.	
	Records Management	
345.	Provide automatic migration of documents between storage platforms as part of the archiving and document lifecycle management process based on triggering events initiated from another system.	
	Workflow	
346.	Support rules-based production workflow routing to process documents through electronic queues.	
347.	Support split screen viewing (a document in one window and another application screen in a second window).	
348.	Provide the capability of routing documents based on user decisions.	
349.	Maintain a log of actions that have been taken on a document (e.g. the routing sequence, notes about problems in processing a document, people who need to review the document and other	

S. No.	Functionality	Compliance Code
	annotations).	
350.	Support a "universal inbox" which is accessible concurrently by multiple users and secure inboxes (access restricted to specific users).	
351.	Support the generation of workflow statistics and status of work items reports.	
352.	Support conditional (if then) logical routing and rendezvous (wait for another action to occur before processing document to a work queue).	
353.	Support parallel routing (routing for the same document to more than one inbox at the same time).	
354.	Be able to be accessed and executed over the intranet, via dial-up access and over the Internet by browser-based clients.	
355.	Be able to be created by trained end-users through graphical tools, using such techniques as "drag and drop".	
356.	Support inter-agency workflow processes.	
	System Administration	
357.	Use graphical tools.	
358.	Have Operating Systems with services such as User IDs, passwords and security levels (for example Windows, Linux etc.).	
359.	Enable remote systems administration over an intranet.	
	Fax	
360.	Be capable of importing and exporting documents to/from the document repository	
	Printer	
361.	Have high volume and high speed print capabilities to cater to the needs of the agency.	
362.	Be able to send print jobs to network printers and to print from individual printers attached to workstations.	
	Web Publishing	
363.	Be able to send print jobs for web publishing to network printers and to print from individual printers attached to workstations.	
364.	Allow browser-based users to enter information over the Internet into forms, and for forms-based information to propagate through the system using the product's workflow or other capabilities.	
365.	Facilitate browser-based users to search for and retrieve, download and print documents in the repository.	
	System	
366.	Support mirrored drives.	
367.	Include back-up capabilities for the document repository and database(s).	
	Collaboration Management	

S. No.	Functionality	Compliance Code
	Collaboration System (CS) Requirements: Correction and Creation	
368.	Allow the users to create new documents and edit existing documents.	
369.	Provide a central secure document repository for storing all the created documents.	
370.	Version control – The user shall have the option whether to create a new version, replace the existing version (provided the document has not been finalized) or create a new document. New versions shall be automatically linked to the original document and higher or lower versions of the document.	
371.	Linking document attachments - The user is able to attach/link multiple electronic documents to form a single "virtual document" which is subsequently managed as a single entity to ensure its integrity.	
372.	Profiling documents with attached images – The user shall be able to profile an original hardcopy document and to attach its image as electronic attachments.	
373.	Launching of applications – The system shall launch the authoring applications (i.e. associated or generic viewer) from within the document retrieval function of the Collaboration System for the purpose of creating, editing or viewing a document.	
	Instant Messaging	
374.	Secure communication (including message encryption)	
375.	Support Instant Messaging clients	
376.	NOT support desktop client software beyond a standard web browser	
377.	Give the user the capability to present documents to session participants through their browser.	
378.	Have the capability to identify the status of the team members, whether they are “Away”, “Out to Lunch”, “Busy” or “On the Phone”. (This enables users to see instantly the availability of other Team Members in joining the conference / Meeting)	
379.	Instantly escalate Instant Messages to conferences and web Collaboration sessions	
	Paging	
380.	Provide the capability for multiple users to collaborate together in a single session simultaneously.	
381.	Allow users to leave and re-join sessions.	
382.	Provide the capability for the users to schedule and hold online meeting with identified team members / participants.	
383.	Automatically alert or send notifications to users on the meeting schedules.	
384.	Be able to display presentation slides for other participants	

S. No.	Functionality	Compliance Code
	during the online meeting through shared web browser (Communication with other participants is provided through audio/video links and chat application).	
385.	Provide whiteboard tools that can be used to clarify meeting issues.	
386.	Allow users the option to share their screens or selected applications. (All users have access to the list of meeting participants)	
	Security	
387.	Provide an individual profile for each Collaboration System user and a facility for managing "permission" associated with read, write, modify, delete and disposal rights and restrict those permissions to designated individuals at the group, document and file classification level.	
388.	Allow the user to electronically designate a document as being finalized (authorized by a named authority) thereby protecting the document from modification.	
389.	Enable administrator and records manager to restrict creation of new files to designated users.	
390.	Provide a strong encryption feature for meeting the requirements for handling Government classified information.	
391.	Have its own self-contained security system and protect the integrity of information within the system throughout each stage of the life cycle of the record.	
392.	Provide an audit log showing changes made to the security parameters.	
393.	Protect against unauthorized access by hiding from the end user, the user ID and password information used for access and prevent unauthorized access to all system tables.	
394.	Use the same password facility as the LAN and must not impose the use of additional passwords to gain access to the system.	
	Retention and Disposal	
395.	Be able to create, maintain, modify and manage retention and disposal schedules indicating the period of time documents are to be retained in an active and inactive state; and to create, maintain, modify and manage a listing with instructions for the authorized Disposal of documents such as destruction or transfer	
396.	Enable administrator and Records Manager to change defaulted retention and disposal designations for individual documents in order to support disposal exceptions.	
397.	Provide on-line assistance and an enabling mechanism to change document status between active, inactive and archival storage.	
398.	Provide a means to identify all official documents due for destruction, within the workgroup according to their authorized records disposal schedules.	

S. No.	Functionality	Compliance Code
399.	Provide a means to delete a document and its attachments from all repository media (including removable media) such that the document and its attachments cannot be reconstructed if such deletion is authorised by CCI	
	Retrieval	
400.	Bookmark frequently used / common documents.	
401.	Enable the user to select one or more document repositories prior to invoking a document search and to present the search results from the selected repositories in a combined manner showing the source repository.	
402.	Enable the user to use intelligent search, such as Boolean and fuzzy search to search on document contents. All searching shall be case insensitive as default, while also allowing case-sensitive searches.	
403.	Provide facilities to ensure that "read, write and modify rights" are restricted to designated individuals for department-wide repository access rights.	
	Thesaurus search	
404.	Enable users to perform thesaurus searches on the document contents using either the English or Hindi interface.	
405.	Provide the ability to select a term in either Hindi or English. A single search would then be performed using the terms provided.	
	Retrieval Presentation	
406.	Provide a facility to retrieve electronic documents and associated attachments from any document repository (or a collection of documents) informing user on location of document (e.g. online, offline, etc.)	
407.	Include the capability to view electronic documents without launching the native or originating application.	
408.	Allow the user to view, retrieve or print electronic documents from a customizable hit list.	
409.	Enable the user to select and retrieve one or more documents from an attached/linked multiple electronic documents (a single "virtual document").	
410.	Provide a mechanism to ensure that the default retrieval strategy shall always retrieve only the most recent version of a document. The system must also provide a facility for the retrieval of any or all earlier versions of an electronic document as requested by the user.	
411.	Provide each user with a list of the most recently edited or profiled documents at the desktop.	
	Check-in / Check-out and Editing of Electronic Documents	
412.	Enable the user to check-in and check-out electronic documents.	
413.	Prevent other users from modifying a checked-out document but allow viewing access by those users.	

S. No.	Functionality	Compliance Code
414.	Provide notification, when a user attempts to access a file that has been checked- out.	
415.	Provide the capability to check-in a document without having to launch the native application.	
416.	Allow the administrator to specify a default "application, and its version, of choice" for editing sessions, where a file format is supported by multiple applications (e.g. BMP is supported by a number of graphics editors).	
417.	Provide the capability to open additional documents into an existing instance of an application	
	Auditing	
418.	Maintain charge in / out history for files, volumes, documents and secondary storage containers.	
419.	Provide the capability to compile statistics and produce management information such as the number of times a document is accessed/processed/updated as well as the number of documents accessed by organizations/groups.	
420.	Maintain and provide reports on revisions to document, access to document and change to document status.	
	Interface	
421.	Provide a Graphical User Interface (GUI) interface or a web-enabled interface.	
422.	Enable a designated individual to access, revise or make additions to online help facilities including the capability to load, maintain and retrieve custom process rules pertaining to using and administering the Collaboration System.	
	Workflow	
423.	Have the capability to route the information to specific participants before posting it for general consumption and can be used to indicate when and where that information will be posted.	
	Email System	
424.	Allow integration with messaging software such as Lotus Notes. The user shall be able to Transfer e-mail messages, their associated documents and attachments between messaging software such as Lotus Note and the system such that e- mail messages can be filed in an Collaboration System repository; and initiate mailing Collaboration System-filed documents from a Collaboration System repository as attachments to an e-mail message	
425.	Provide a facility for automatically capturing e-mail message attachments (sent and received).	
426.	Use document name and not system generated name that may or may not be arbitrary filename for the capture of emails and email attachments (for example John Smith and not foxman@domain).	

S. No.	Functionality	Compliance Code
	Replication	
427.	Provide the capability for users to work with the document offline and synchronize automatically when the users are online.	
428.	Enable replicated repositories – the technical architecture provides replicated repositories, which are duplicates of a repository that can be distributed to different geographical locations.	
	Knowledge Management	
429.	Have the capability to support the concept of a "group memory". (Store the intellectual capital and can be reuse by other users).	
430.	Have the capability to reuse the knowledge and best practices adopted by the users in the Collaboration System.	
431.	Bookmark for frequently used knowledge and best practices adopted by the users in the Collaboration System.	
	Tracking	
432.	Provide the capability for the users to view and track the status and milestones of the task.	
433.	Provide the capability to alert and notify the users regarding the expiring of due date.	
	Multimedia Support	
434.	Provide the capability to support for MPEG, JPEG, AVI, Flash TM QuickTime TM, GIF, WAV, AU and MS Windows bitmap etc.	
	Virtual Briefcase	
435.	Provide a virtual workplace / environment for users to view, edit and create information / documents.	
436.	Provide a "virtual room" construct to provide multiple shared virtual spaces for collaborative use of researching, planning, communications and analysis tools.	
	Additional Functional Requirements	
437.	Provide the capability for users to add in comments / suggestions to the working documents. (Only for authorized users)	
438.	Allow users to send messages in respond to various events during a process. For example, ability to notify a system operator if the process fails or e-mail a report produced by the process if it succeeds.	
439.	Enable the format for the email notification to include the title of the event.	
440.	Notify the respective team members regarding an expired deadline or if a workflow was fulfilled successfully through a triggered notification process.	
441.	Categorize email notifications into at least two categories such as Urgent email and Normal email.	
442.	Ensure that the notification system is easy to use, has a point and click interface, and can be used to define notification	

S. No.	Functionality	Compliance Code
	escalation chains. When an action fires, the notification will continue to escalate at the specified time intervals, until the desired individual responds to the event.	
443.	Allow the users to customize their notification and provide details of every aspect of the notification process and historical reporting for use in capacity planning.	
444.	Be able to offer a wide range of options for sending status messages for the process, including the ability to send files produced by the process.	

4.18 Knowledge Management

Knowledge portal will be created as a platform for knowledge creation and sharing among employees of CCI.

The KM system, inter alia, will use the resources such as:

- Repository of cases
- Research Papers
- Directory of Skills and Experts
- Job Description Table
- Role Table
- Skills Table
- Initial network of communication Forums
- Glossary of Terms
- Comprehensive Partially Annotated Bibliography
- A list of all knowledge assets
- All current job descriptions
- A detailed organizational chart
- List of workers' training and testing histories
- A list of all approved training being utilized
- An overview of the future direction of the organization
- A list of current skill definitions, if any
- Procedural manuals
- Orientation materials

Collect and transform tacit knowledge into explicit knowledge by representing and structuring it and in knowledgebase for providing access to users in a friendly and adaptable form of visualization.

The system will use the knowledge based reasoning and content categorisation on the content gathered from the resources and distribute in user acceptable format which will assist in cases of Section 3, 4, 5 & 6.

4.18.1 Technical Specifications

S. No.	Functionality	Compliance Code
1.	**User Interface**	
1.1	Have the capability to support the concept of a "group memory". Store the intellectual capital that can be reused by other users).	
1.2	Have the capability to reuse the knowledge and best practices adopted by the users in the Collaboration System.	
1.3	Bookmark for frequently used knowledge and best practices adopted by the users in the Collaboration System.	
1.4	Ability to provide control and distribution of the organisation's policies and procedures	
1.5	Ability to locate any information easily, including workflow processes and eForms	
1.6	Ability to provide access to internal and external users for quick location of content, processes and eForms using keywords and meta data	
1.7	Ability to apply consistent document tagging through attributes and category classes that support inheritance	
2.	**Domain Ontology Features**	
	Taxonomies	
2.1	Provision to define taxonomies providing navigation device for browsing the content repositories, representing intuitive semantics of the user information requirements.	
2.2	Ability to define class predicates in the form of queries comprising information object property values or as full text queries comprising key word and/or phrases.	
2.3	Ability to organize into hierarchical structures comprising any number of categories, usually corresponding to occurring information object property value (e.g. a name directory) with the maximum number of categories equal to the cardinality of the property value domain.	
2.4	Ability to automatically categorise information objects based on arbitrary functions defined on object property values and/or content and implemented as an arbitrary analytical algorithm	
2.5	Ability to define and use analytical algorithms that provide for automatic categorisation of formatted data objects, textual objects, as well as multimedia objects, such as audio, images and video frames.	
2.6	Ability to use knowledge-based reasoning function. Using an inference engine to provide for the actual categorisation of information objects.	
	Conceptual trees	
2.7	Provision for conceptual trees as a categorisation device used in conjunction with full text queries providing means to define	

S. No.	Functionality	Compliance Code
	concepts on the basis of its hierarchical relationships with other concepts, key words, and phrases. Usually conceptual trees allow for the full text query relevance ranking.	
	Semantic Nets	
2.8	Ability to use Semantic networks to represent binary 1:1 relationships, expressed usually as named arcs of a directed graph, where vertices are information objects belonging to any of the information object classes.	
2.9	Semantic nets may be constructed over an arbitrary number of information object classes and binary relationships.	
	Semantic Data Models	
2.10	Ability to use semantic data models allowing for definition of structural as well as behavioural semantics. Class Association Diagrams provide easy to read, intuitive semantics closely matching the mental models of the users.	
2.11	Ability to provide a navigation facility allowing the user to transverse the network of specified object associations and to view/retrieve the corresponding object sets.	
	Hyper-text links	
2.12	Ability to create ad hoc relationships between content artefacts in the repository.	
2.13	Ability to provide the hyper-text links to support referential link semantics that may exist among the information objects belonging to arbitrary object classes existing in the content repository and	
2.14	Ability to use hypertext links as annotation tool to express, possible transient, referential relationships of information objects stored in the content repository.	
	Time Modelling	
2.15	Ability to use time valued properties for search and automatic categorisation operation, in knowledge descriptions and content characterization. Precise rules must be established as to representation and treatment of temporal properties to be comprised in a knowledge management system.	
2.16	Ability to use time modelling to represent the declarative and procedural knowledge representation.	
	Knowledge-based reasoning	
2.17	Ability to use the knowledge based reasoning knowledge and content categorisation and distribution.	
	Process graphs	
2.18	Ability to use process graphs like to enable the workflow management engine to properly assign tasks to KMS actors. The process graph representation should comprise a set of process metrics and, possibly, performance constraints and exception	

S. No.	Functionality	Compliance Code
	conditions.	
3.	**Content Repository features**	
	Extensible Markup Language (XML)	
3.1	Ability to use XML for exchange of data between information systems as well as for storage and retrieval of complex, multimedia objects in content repositories.	
	Resource Description Facility (RDF)	
3.2	Ability to define complex relationships between documents or data.	
3.3	Ability to use RDF for mapping UML semantics into the content repository data models. RDF schema is used as a template to define annotation in RDF syntax.	
	File Systems	
3.4	Ability to use File systems in multimedia content repositories to serve as containers for large content objects represented as files.	
3.5	Ability to use file systems technique for mapping content onto diverse hardware storage devices in order to exploit their inherent characteristics. E.g. for permanent non-modifiable storage of electronic documents an optical storage device may be used.	
3.6	Ability to compose file systems into storage hierarchies usually controlled by the document management software.	
	Hierarchical Storage Management	
3.7	Provision for the hierarchical storage management to control allocation of storage space available in a hierarchy of storage devices to large content object files.	
	Database Management System (DBMS)	
3.8	The provision, among others, for Object-relational database management systems as an implementation platform for the domain ontology management functions and the content management functions.	
3.9	Ability to use DBMS for storage of all KMS directories and control blocks, for representation of the domain ontology data model, and for storage of content object files and attributes.	
3.10	Ability to use main memory relational database management systems to store frequently used ontology structures as well as to provide a platform for representing data structures representing facts in knowledge-based reasoning algorithms.	
	Version control	
3.11	The versioning mechanism should allow for transparent identification (incremental revision number) and storage (either full version or increments) of particular versions of content and content object properties.	
	Rendering	
3.12	Ability to render the content in web based browser through	

S. No.	Functionality	Compliance Code
	renditions including HTML and XML, as well as PDF and other well know formats besides the native format.	
4.	**Knowledge Dissemination features**	
	Push Technology	
4.1	Ability to provide facilities for automatic supply of selected content objects to a predefined group of recipients (a role), who are usually the actors (knowledge workers, intelligent agents);	
	Content Object Properties	
4.2	Ability to characterize the principal object properties, such as object identifier, origin, author(s), date, etc., as well as provide information, in the form of key words, characterizing the content.	
	Full Text	
4.3	Provision for full text retrieval techniques, used in conjunction with conceptual trees.	
	Knowledge Map Graphs	
4.4	Ability to use advanced graph construction and manipulation techniques to provide the required ergonomic level of the KMS user interface and employ knowledge graphs in a query mode, for navigation within the semantically meaningful structures and for browsing the associated content.	
5.	**Content Integration features**	
5.1	Provision for all entities, regardless of their character (structural, procedural), participating in the content integration process must be accessible via the knowledge map graph, or via other existing access path to the content repository.	
5.2	Provision for any of the integrated content objects, constrained by the corresponding descriptions of the content repository schema, to be either physically stored in the repository as a content object (snapshot, refreshable), or to be dynamically materialised at the reference time. Usage of the above integration modes should be entirely transparent to the user.	
	Files	
5.3	Files feature among candidates for content integration, due to the widely diffused usage of file systems as repositories of large, multimedia content objects. Little, or no, analysis of the multimedia objects content, apart from the automatic categorisation analysis, is performed during the integration process.	
	Database Query	
5.4	Provision for heterogeneous multi-database query and integration techniques, as well as the homogenization of heterogeneous data models	
5.5	Ability to query a single database to materialise the required content to be further exploited in the KMS context, either as an element of a content object stored in the repository, as a virtual	

S. No.	Functionality	Compliance Code
	content object materialised on-the-fly.	
	Business Intelligence Systems	
5.6	Ability to integrate the relevant knowledge delivered in Data warehouses and OLAP system into the KMS.	
	Business Application Systems	
5.7	Ability to access other application system reports as content objects, or their elements, via the KMS content repository.	
	Intelligent Agents	
5.8	Ability to use intelligent agents that carry out some set of operations on behalf of a user or another program with some degree of independence or autonomy, and in so doing, employ some knowledge or representation of the user's goals or desires.	
	Document Management Systems	
5.9	Ability to integrate with Document management systems for content infrastructure directly relevant to the users and integrating electronic documents and image-based information into the content repositories as principal factual knowledge artefacts.	
	Web Pages	
5.10	Ability to access data volumes that is available on web pages for external knowledge acquisition and keeping it up-to-date.	
6.	**Collaboration Features**	
	Message Exchange	
6.1	Provision for use of Instant messaging (tacit to tacit knowledge transformation) supporting the knowledge production process. Ability to categorise and store the electronic messages in the content repository.	
	Discussion Forums	
6.2	Ability to categorise the relevant and valuable statements and comments of discussion forums and store them in the content repository and measures (e.g. attributed to the originating sources).	
	Knowledge Engineering	
6.3	Provision for analytical support for knowledge-based reasoning applications and intelligent agents to glean the expert knowledge out of individual (outstanding knowledge workers).	
6.4	Provision for the process of obtaining expert knowledge, required to build knowledge-based (or expert) applications,	
6.5	Provision for the formal knowledge representation both for declarative and procedural knowledge	
	Workflow Management	
6.6	Provide for interaction and integration between the KMS workflow management processes, and the workflow management supporting the business processes of an organisation.	

S. No.	Functionality	Compliance Code
	Internet/Intranet	
6.7	Ability to integrate the content resources that are available on the Net	
6.8	Ability to publish information relevant to organization's stakeholders	
7.	**Security features**	
7.1	Ability to integrate such security features as electronic signature, encryption, access control and user authentication which are provided for the entire system of the organisation.	

4.19 E Discovery

E Discovery solutions should deliver rigorous and efficient electronic discovery processes to meet evolving and complex legal obligations. The solution should help CCI in following stages of E Discovery:

a. Identification of documents
b. Placing identified documents on legal hold
c. Collection of documents and create a folder for review by legal division
d. Assist in review of the documents for completeness and relevance
e. Production of the documents in desired format for legal representation

4.19.1 Technical Specifications

S. No.	Functionality	Compliance code
1	**Legal Hold Module**	
1.1	Ability to create and send same or different hold notices to relevant custodians and system administrators via email immediately or scheduled for delivery.	
1.2	Ability to create and send reminder email notices scheduled for delivery to non-responsive custodians, eliminating the need for manual follow-up	
1.3	Ability to create and send escalation email notices scheduled for delivery to a custodian's manager if a custodian is not responsive	
1.4	Provision to save hold notices as templates in the a notice repository for reuse, enabling administrators to achieve greater consistency and efficiency across the legal hold process	
1.5	Provision for Automated tracking and reporting to enable administrators have immediate visibility into the status of all legal hold notices across all cases through a single pane of glass.	
1.6	Ability to enable drill-down by case to view the status across all custodians, including those who have received and responded to their hold notices, and those who haven't.	

S. No.	Functionality	Compliance code
1.7	Ability to release one or more custodians from a hold with one simple click of a button and send release notices automatically to targeted custodians.	
1.8	Provision for custodian portal to enable custodians have access to individual portals that summarize their active, pending, and released holds in a single view, enabling them to easily track all their legal obligations in one place	
1.9	Custodian survey—Surveys containing single-choice, multiple-choice, or free form text questions can be created and issued to key custodians so administrators can easily capture information critical to a case, thereby expediting the interview process. Surveys can also be saved as templates to the Notice Library and reused	
1.10	Survey response report—Survey responses are automatically captured and immediately available for analysis both in a summarized format and by individual custodian via easy-to-read charts and graphs.	
1.11	Ability to dynamically populate the custodians into the system from Active Directory /LDAP. Employees purged from the Directory may still be retained in the system as custodians, ensuring a defensible record of all legal hold activity.	
1.12	Ability to maintain and track every legal hold action, such as hold notice, response, confirmation, escalation, and release, via an exportable report, creating a complete and detailed audit trail	
1.13	Capability to route legal hold responses to a separate server that provides access to all custodians, ensuring that the primary system server is accessed by designated legal and IT users only.	
1.14	Provisions for users to issue legal holds, and then collect, process, analyse, and review case data all within the same application, ensuring a defensible e-Discovery process	
2	**Identification and collection module**	
	Identification	
2.1	Provision for users to interactively build a map of custodians and data sources enabling them to identify all the potential sources of data for a particular matter	
2.2	Ability to search and browse the data sources by group ,custodian, or data source type	
2.3	Ability to make changes to the map directly and immediately using intuitive and user-friendly Web-based interface	
2.4	Provision for a single repository to keep track of an employee's information so that changes, such as email address, name, or title, can be maintained in the e-Discovery workflow and automatically updated	
	Collection	

S. No.	Functionality	Compliance code
2.5	Ability to collects data to a preservation data store directly over the network.	
2.6	Ability to configure and initiate collections by browsing to specific data sources and folders using the graphical user interface	
2.7	Allows secure on-site collections from laptops, PCs, and files shares onto any external hard drive when network collection is not feasible.	
2.8	Provision for configuration parameters to provide the flexibility to copy the data onto a pre-defined network location or a USB drive	
2.9	Enable targeted collections by filtering via metadata fields such as owner/author, date range, and file type. Users can specify criteria via a GUI interface	
2.10	Ability to filter collections by key words. Providing administrators the option to leverage existing source indices to utilize federated search-enabled key word collections from data sources behind the firewall or in the cloud	
2.11	Enables targeted collections from the archives by providing metadata and key word filters that use the archive's existing index data classification tags. Provide GUI interface to enable users to specify collection criteria.	
2.12	Ability to run search-only tasks against archived sources, preview sample files, and run date range and custodian-based analytics on the results, enabling early analysis on archived data without the necessity to collect.	
2.13	Ability to allows users to collect the full range of collaboration document types including blogs, wikis, calendar items, announcements, discussions, and surveys, and render them in context.	
2.14	Ability to automatically schedule network collections to run at a user-defined time and date, providing flexibility while also freeing administrative resources.	
2.15	Ability to collect only new or modified data using the same collection parameters as the original collection on a recurring basis, saving users time from having to set up follow-on collections from scratch.	
2.16	Ability to save commonly-used collection settings, including specific directories, filters, preservation stores, and custodian assignments, for reuse during future collections.	
2.17	Ability to automatically perform separate MD5 hashes of every file before and after collection while preserving all metadata, ensuring every collection is always forensically sound and defensible. Reporting should be available on all files collected as well as every file filtered out.	

S. No.	Functionality	Compliance code
2.18	Ability to automatically record collection details for every custodian and data source, including the volume, time, and status of the collection, providing real-time visibility into the collections process.	
2.19	Ability to securely decrypt and collect documents on the fly.	
2.20	Provide a complete portfolio of analytical charts and tables that displays volumes and types of data that have been collected by custodian. Ability to export charts and tables in CSV or XLS formats to present real-time visibility into what has been collected or missing, facilitating immediate remediation critical for defensibility.	
3	**Processing and Analysis**	
	Processing	
3.1	Ability to enable users to interactively filter data by custodian, date, strong file type, and file size prior to processing.	
3.2	Ability to summarise and visually present overall document set characteristics and present detailed analysis by custodian, timeline, and file type to confirm that all case data has been collected.	
3.3	Ability to processes and analyse different file types from data stores and network file shares including Microsoft Office® and PDF documents, various email formats such as PST, NSF, MBOX, OST, and EMLX, attachments etc. Ability to translate text in image files to searchable content with integrated OCR.	
3.4	Ability to provide full Unicode compliance and support different Indian languages. Enable automatic language identification of documents and provide exact document counts by language type across the entire data set.	
	Analysis	
3.5	Enable reviewers to easily identify and view emails, attachments, and loose files with similar content to the document under review using a dynamically configurable similarity threshold.	
3.6	Ability to automatically organize documents into specific topics enabling users to quickly analyse all documents related to a particular subject.	
3.7	Ability to analyse individual and group-to-group communications within the organisation or to customers, suppliers, and partners. Users can easily access a list of top custodians for a search or monitor communications between divisions.	
3.8	Ability to leverage natural language algorithms to analyse noun phrases, which help users uncover secret project names and code words that may be relevant to a case or investigation	

S. No.	Functionality	Compliance code
3.9	Enable reviewers to easily identify, view, and tag near-duplicate emails, attachments, and loose files and compare near-duplicate documents with differences automatically highlighted.	
	Search	
3.10	Ability to provide matching key word variations prior to running a search enabling users to selectively include relevant variations or exclude false positive variations.	
3.11	Enable real-time search result filtering for individual queries or variations and allow users to sample the filtered documents.	
3.12	Ability to provide comprehensive reporting that documents all search criteria and provides detailed analytics of the results.	
3.13	Ability to run multi queries simultaneously, to reduce the time needed to evaluate the effectiveness of key word searches.	
3.14	Ability to construct advanced searches based on numerous metadata and derived fields.	
3.15	Ability to support both stemmed and un-stemmed (literal) searches and provide user the capabilities including Boolean, wildcard, fuzzy, nested proximity searches, and prediction scores.	
3.16	Ability to automatically group search results by metadata fields such as tag, sender domain, document type, custodian, language type, and prediction score and display exact hit counts across the entire search result set for every filter.	
3.17	Ability to perform concept search	
3.18	Enable users to contextually refine the concept search by previewing the most frequently occurring terms and selecting only the relevant ones.	
3.19	Ability to let users to dynamically construct searches by exploring terms and linking them to form comprehensive and relevant concepts in a visual interface	
3.20	Ability to automatically document the related terms included in each concept search.	
4	**Review and Production**	
	Review	
4.1	Ability to view documents in a near-native format without requiring each application to be loaded on a reviewer's work station. Both text search and hit highlighting within documents are available, increasing reviewer productivity.	
4.2	Ability to redact documents in multiple colours, applies reason codes, and verifies redactions prior to production. Reviewers should be able to redact specific text, pages, or areas within a document. Enable reviewers to navigate through each redaction within a document and perform quality control checks to verify accuracy.	

S. No.	Functionality	Compliance code
4.3	Ability to delivers a flexible and intuitive workflow that leverages the intelligence of expert reviewers to train the software on tagging criteria, automatically generate predictions, and analyse accuracy for rapid review.	
4.4	Ability to provide sophisticated analytics by criteria such as custodian, discussion, concept, and participant to ensure the selection of a highly relevant initial training set.	
4.5	Ability to automatically provide a prediction scores for the document under review, transparently displaying content and metadata relevant to the prediction.	
4.6	Ability to provide a set of built-in quality control capabilities allowing users to measure review accuracy, identify inconsistent tagging, highlight disagreements between reviewers, and automatically compare predictions and human decisions to assess and improve review accuracy.	
4.7	Ability to provide intuitive statistical sampling tools to select an appropriate random sample based on the accuracy requirements of the case.	
4.8	Enable users to streamline the review of cross-matter issues by using templates to import and export prediction models across cases.	
4.9	Allow reviewers to easily identify, view, and tag near-duplicate emails, attachments, and loose files. Capability to compare near-duplicate documents with differences automatically highlighted.	
4.10	Allow reviewers to easily identify and view emails, attachments, and loose files with similar content to the document under review using a dynamically configurable similarity threshold so that the process of reviewing similar documents together can provide full context for the document under review, and ensure greater tag consistency.	
4.11	Ability to tag individual or sets of documents using a multi-layer tree structure to direct reviewers into key decision points, preventing errors and minimizing the number of clicks needed to accurately tag a document.	
4.12	Ability to tag items (email, loose files, files embedded within documents, and attachments) separately from one another. Tag sets may be defined to allow their tags to be applied to individual items or to an entire document.	
4.13	Enable administrators to automatically allocate documents into review folders using flexible allocation rules; auto-batching streamlines the process of creating review sets for easier case management.	
4.14	Enable users to monitor the completion of review sets and see which review folders are currently checked in or out by any reviewer so that case administrators can control access to the	

S. No.	Functionality	Compliance code
	review folders and stop or complete a review that is in progress.	
4.15	Ability to automatically identify and display related documents, such as near-duplicates, documents with similar content, documents contained in the same discussion threads, and attachments to the document under review	
4.16	Ability to highlight search terms in emails, attachments, and files within the near-native viewer, allowing reviewers to quickly navigate to key words across one or more searches (e.g., terms from previously executed privilege and responsive searches).	
4.17	Enable users to log off then later resume their work with the exact document and screen settings displayed prior to logging off, eliminating delays associated with resetting screen settings	
4.18	Ability to provide document review progress for a case in an automatically generated graphical report. The report can be customized to report on folders, tags, dates, and users and facilitate administrators to easily monitor the real-time status of cases using a variety of parameters	
4.19	Enable case administrators to easily manage reviewer accounts, including user name, password, role, and access to tag and production privileges. All reviewer actions, such as login, logout, search, tag, print, and export, are tracked, providing a full, reproducible audit trail.	
4.20	Enables case administrators to dynamically increase the number of concurrent reviewers by adding capacity on-demand in order to meet tight deadlines and handle the largest cases.	
	Production	
4.21	Ability to produce documents in native, image (TIFF or PDF), and mixed mode formats (e.g. Excel spread sheets in native, but all others as images). Flexible export options allow for multiple metadata formats (EDRM XML, DAT, CSV, etc.), "reduplicating" of data by custodian, and preservation of original folder hierarchies.	
4.22	Ability to automate the sequential numbering of documents with Bates Stamps and support custom labelling of produced documents using headers and footers	
4.23	Enable review teams to create production sets using the same folder features utilized during review, enabling a collaborative approach to building accurate production document sets.	
4.24	Provision for sharable export templates and pre-mediation of issues which eliminate manual steps, reduce errors, and enable case administrators to pre-emptively address issues resulting in faster export and production	
4.25	Enable batch productions at any point in the eDiscovery process for users to track the progress of each production in real-time and view produced document sets in the exact format provided to outside parties	

S. No.	Functionality	Compliance code
4.26	Provides customizable load file creation during export extending the export options for multiple metadata formats including CSV, DAT, EDRM XML	

4.20 Video Conferencing

Video conferencing should provide two-way interactive audio and video communications between two or more end points to provide simultaneous (real-time) communications among people across different locations through voice / audio and smooth full-motion colour video.

S. No.	Functionality	Compliance code
1.	Ability to connect simultaneously users equivalent to the number of licenses purchased, irrespective of their location	
2.	Ability to work on any network MPLS, LAN, WAN, VPN, Home Broadband and wireless data cards and any audio- video peripherals	
3.	Ability to get anyone connected from anywhere across the world over internet, be it office, home, hotel, airport or even car.	
4.	Compatible with a wide variety of industry standard PC audio and video conferencing equipment	
5.	Ability to mix and match ordinary webcams, conference room pan-tilt-zoom (PTZ) cameras, HD, PC and laptop built-in cameras, even conference participants with no camera whatsoever, all in the same online meeting	
6.	Ability to call any of the hardware video conferencing devices from Polycom, Tandberg, Lifesize etc. into the same conference over the optional H.323 bridge (The H.323 standard addresses call signalling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences	
7.	Provision for just one STATIC IP at central Location and no separate Static IP/Public IPs are required for the rest of the connecting location; anyone should be able to connect into the video conference meeting on the move from anywhere, even using High Speed Data Cards while travelling.	
8.	Provision for scalability and upgradeability (Right from Standard Definition Video Conferencing to High Definition 720p, Full High Definition (1080pVC) and Scalable to High End Telepresence.	
9.	Ability to share PowerPoint, Word, Excel, PDF Etc., along with Movie Files and all types of Applications including Desktop and ability to record Video conference meetings for later use and training purposes.	
10.	Provision for the video output screen as divided to accommodate	

S. No.	Functionality	Compliance code
	the sites to be simultaneously shown in the conference.	
11.	Provision for the voice activated multi-site switching feature which on being activated makes the output screen to appear in full screen mode and show the site/person which is speaking at present thus enabling to have a multi-conference video conferencing as it keeps the focus highlighted on the person who is speaking at the given moment.	
12.	Provision for SIP-based videoconferencing (soft-switch gateway), SMS and VoIP enabling Voice only conference members to join the video conference meeting: - Ability to allow users to connect to SIP based Video Conference devices Like VIDEO PHONES or Polycom, Tandberg, Aethra, Sony Etc.) into the Video Conference via their wire-line or mobile phones. - Ability to connect to SIP Phones enabling participants to dial into either a toll free or local access number to connect into a Video Conferencing meeting.	
13.	Provision for SMS & VoIP to connect a GSM Modem to your Video Conference Server and the Conference invitation can be sent through SMS to the Conference Participants mobile number. The VoIP module allows participant to Connect or call any phone into the Video Conference System using VOIP Services at cheaper rates (the VoIP service id can be taken from Local VOIP service provider)	
14.	Ability to send Video Outputs to External displays like Plasma or LCD TV's using Decoder card.	
15.	Provision for dynamic network bandwidth management to protect bandwidth and optimize the use of network resources based on the class of user, location and capacity of the underlying network; this should ensure quality of experience (QoE) to the end-user, and quality of service (QoS) to the administrator.	

5. Hardware Specifications

Response to Specification

- **C** – Compliant
- **NC** – Not Compliant

5.1 DMS Server

S. No.	Features	Specifications Required	Compliance Code
1.	CPU	Intel Xeon E5-4650, 2.7 GHz 8 core processor or better (supplied with two processors as standard) with 20 MB L3 cache upgrade to four Processor	
2.	Chipset	Intel OEM	
3.	Motherboard	OEM / Intel Original Motherboard.	
4.	Slots	Minimum 5 PCI Express Slots	
5.	Memory	64GB 1600 MHz DDR3 RAM upgradable up to 1.0TB with support of memory mirroring, ECC	
6.	HDD Slots	Minimum 4 nos& upgradable to 16 Slots. Should Support SAS/SATA/SSD in same Slots	
7.	Hard Disk Drive	2 x 300 GB, 15000 rpm SAS Hot Plug or better	
8.	RAID Controller	6 G SAS Controller with 1GB Flash cache and support for RAID 0,1,5,10	
9.	Video Controller	To support VGA with Min 16MB RAM or above with min 16M colors	
10	Ports	2 USB Port, 1 Serial Port, should have dedicated Internal USB ports for Hypervisor	
11	Cabinet	Rack Mounted, Maximum 2U	
12	Certifications	Windows, Red Hat or Novell certified, Vmware, hyper-V, KVM Compliance & Support	
13	DVD ROM	8x or better DVD ROM Drive	
14	Power Supply	Redundant Power Supply	
15	Fan	Redundant Fan	
16	Networking	Dual LAN (10/100/1000) Network Card with asset tracking Feature and security management, remote wake up and dual 10 GbE copper or fiber options	
17	Security	Power-on password, administrator's password, Trusted Platform Module	
18	Management	UEFI, Integrated Management Module with separate port, Predictive Failure Analysis, Light Path Diagnostics/Equivalent, Automatic Server Restart Server should be supplied with OEM Server	

S. No.	Features	Specifications Required	Compliance Code
		Management software	
19	External Storage Connectivity	2 * 8 Gbps FC HBA cards in Redundant configuration per server for connectivity to SAN switches	
20	Keyboad and Mouse	Connected to KVM	
21	Connectors and Cables	All necessary network & power cables & connectors of OEM make only are to be provided	
22	Operating System Support	Window, Linux	
23	Operating System & Cluster software	Latest full 64 Bit RHEL AS/ Unix/Windows with cluster support· (Active) – (Active) cluster· System should also support partitioning & consolidation features.	
24	Load balancing & Path Failover	Required software for load-balancing & path failover should be provided	
25	Warranty Period	3 year onsite warranty with 24x7 The support should be directly from OEM	

5.2 Database Server

S. No.	Features	Specifications Required	Compliance Code
26.	CPU	Intel Xeon E5-4650, 2.7 GHz 8 core processor or better (supplied with two processors as standard) with 20 MB L3 cache upgrade to four Processor	
27.	Chipset	Intel OEM	
28.	Motherboard	OEM / Intel Original Motherboard.	
29.	Slots	Minimum 5 PCI Express Slots	
30.	Memory	64GB 1600 MHz DDR3 RAM upgradable up to 1.0TB with support of memory mirroring, ECC	
31.	HDD Slots	Minimum 4 nos& upgradable to 16 Slots. Should Support SAS/SATA/SSD in same Slots	
32.	Hard Disk Drive	2 x 300 GB, 15000 rpm SAS Hot Plug or better	
33.	RAID Controller	6 G SAS Controller with 1GB Flash cache and support for RAID 0,1,5,10	
34.	Video Controller	To support VGA with Min 16MB RAM or above with min 16M colors	
35.	Ports	2 USB Port, 1 Serial Port, should have dedicated Internal USB ports for Hypervisor	

S. No.	Features	Specifications Required	Compliance Code
36.	Cabinet	Rack Mounted, Maximum 2U	
37.	Certifications	Windows, Red Hat or Novell certified, Vmware, hyper-V, KVM Compliance & Support	
38.	DVD ROM	8x or better DVD ROM Drive	
39.	Power Supply	Redundant Power Supply	
40.	Fan	Redundant Fan	
41.	Networking	Dual LAN (10/100/1000) Network Card with asset tracking Feature and security management, remote wake up and dual 10 GbE copper or fiber options	
42.	Security	Power-on password, administrator's password, Trusted Platform Module	
43.	Management	UEFI, Integrated Management Module with separate port, Predictive Failure Analysis, Light Path Diagnostics/Equivalent, Automatic Server Restart Server should be supplied with OEM Server Management software	
44.	External Storage Connectivity	2 * 8 Gbps FC HBA cards in Redundant configuration per server for connectivity to SAN switches	
45.	Keyboad and Mouse	Connected to KVM	
46.	Connectors and Cables	All necessary network & power cables & connectors of OEM make only are to be provided	
47.	Operating System Support	Window, Linux	
48.	Operating System & Cluster software	Latest full 64 Bit RHEL AS/ Unix/Windows with cluster support· (Active) – (Active) cluster· System should also support partitioning & consolidation features.	
49.	Load balancing & Path Failover	Required software for load-balancing & path failover should be provided	
50.	Warranty Period	3 year onsite warranty with 24x7 The support should be directly from OEM	

5.3 Blade Server

S. No.	Features	Specifications Required	Compliance Code
1	Form Factor	Blade	
2	CPU	2 x Hex Core x86 based CPU E5-2620, 2.0 GHz ,15MB L3 Cache	

S. No.	Features	Specifications Required	Compliance Code
3	Cache L3	15MB of L3 Cache or better	
4	Chipset	OEM Chipset	
5	Memory	32GB DDR-3 1600 MHz DIMMS Memory Upgradeable to 512GB. Minimum 24 slots and Min 50% should be vacant after configuring the 128GB RAM for future Expansion	
6	Memory protection support	ECC, Memory Mirroring, Memory Sparing, chipkill/advanced ECC	
7	RAIDControllers	Integrated Hardware Raid Controller to supports Hardware Raid RAID 0, 1, 5, 6 with 1Gb flash cache using Optional Upgrade Should Support CacheVault flash cache protection using Optional upgrade to avoid the possibility of data loss or corruption during a power or server failure iand transfer data to NAND Flash	
8	Disk Drives	Shoud Support 2 nos of SAS & 4 Nos of SSD Disks should be supplied with 2 x 600GB 6Gbps10K SAS Hard Disk Drive	
9	Graphics Controller	16MB SDRAM Minimum	
10	Ethernet Adapter	Server should be configured with 4 Number of 10G Converged ports and should have the vNIC functionality. Should support FCOE and ISCSI functionality.	
11	Fiber Channel HBA Connectivity	Should Support Dual Port 8Gbps Fiber Channel Expansion Adapter. PCIe slot should also support 16Gbps Fiber Channel ports in future for further upgradability	
12	I/O Expansions	2 x PCI Express 3.0 interface with minimum 80Gbps bandwidth support per Slot to support 40Gbps ethernet ports in future	
13	Warranty	3 year onsite warranty with 24x7 The support should be directly from OEM	
14	USB	Minimium one external port	
15	Failure Alerting Mechanism	The server should be able to alert impending failures on maximum number of components. The components covered under alerting mechanism should at least include Processor, memory and HDDs, POST.	
16	Server Management Software	Server should be supplied with OEM Server Management software	

S. No.	Features	Specifications Required	Compliance Code
17	OS Support	Microsoft Windows Server 2008 R2, Windows Server 2012, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 11, VMware ESX Server	

5.4 Blade Chasis

S. No.	Features	Specifications Required	Compliance Code
1	Form Factor	Max 10U Rack mounted Chassis to house at least 14 Compute Nodes of half height or half Wide. Chassis configured should not only support current generation of processors but should support future processor technology up to 5 years or more. The should support with fully configured chasis with all the blades with 135 Watt CPUs with no limitation and future also.	
2	Blade Bays	Per Chasis minimum 14 Half height/Wide or half height/wide Slots to accommodate the 2 socket blades and 4 Socket Blades	
3	IO Modules	Suficient I/O bays to support switches for Min Four 10G Ethernet ports and 2 nos of FC ports in 2 Socket Blade. The bays should Support Coverged, FC, Infiniband, Ethernet 1G/10G Switches	
4	Ethernet IO Module (10GB)	Minimum 2 nos of 10Gbps Converged switch with L2 and L3(VRRP) capabilities to support 4 Ports in Dual socket server and 8 ports in quad socket Server , Should having VM ready open standards and support vNIC capabilities, The Minimum number of uplinks 10 nos- 8 x 10Gbps(Omni Ports to support 8Gbps FC and 10Gbps Ethernet & 2x 1Gbps to support legacy) needs to be populated. If vendor is providing the top of Rack switch then Proposed switch should be configured in the way so that there is no single point of failure and the total uplink bandwidth per server port is at least 10 Gbps for proposed servers. In the Switch total no of Ports should be Total server count ports along with additional 10 nos of Uplink ports needs to be configured. All 1Gbps and 10Gbps uplink ports should be active and configured with necessary SFPs and	

S. No.	Features	Specifications Required	Compliance Code
		cables(Minmum 5Mtr Length)	
5	Fibre Channel IO Module	The proposed Chassis should support Dual FC switch with support for both 8Gb and 16Gb FC SAN Switches. SFP should be supplied along with the switch. And should be configured with 2*8G FC Switches with Min 6 Uplink ports	
6	Midplane	Chassis should have a highly reliable mid plane for providing connectivity to the compute nodes and other components such as Power supply, I/O switches, FAN etcin a highly reliable manner. Blade Enclosure Mid plane should be completely passive with no active components to meet all reliability requirements or there should be dual redundant Midplane in case active midplane is proposed. In the backplane if OEM is not able to support the upcoming 16Gbps FC and 40Gbps Ethernet Technology, then Vendor has to give undertaking that they will do FOC upgrade of the backplane on the launch of the same.	
7	Power Modules	Redundant power modules should be able to provide N+N or N+1 redundancy. Power supplies configured should be 80 PLUS Platinum certified. All the Power supplies to be configured. The power supplies should have option to be connected to Single phase or 3 phase AC power supply with respective PDUs. The power supplies should be confirmed for the N+N redundancy for the offered Config	
8	Cooling FANs/Blowers	Chassis should be configured with sufficient Hot Swap & Redundant variable speed rear access blowers/ fan Modules to supports fullly configured Chasis Blades with the highest clock speed CPUs for quoted Series	

S. No.	Features	Specifications Required	Compliance Code
9	Chassis Management Module	Integrated two redundant chassis Management Modules providing IP based management of the compute nodes and vital elements like FC and Ethernet Switches and should be configured in automatic failover mode • Should allow Role based access and Support up to 32 simultaneous sessions • Should Support Multi Chassis Monitoring • Remote administration without External KVM Console • Should use the Dedicated integrated Controller/port on compute Nodes to manage the Nodes and other components • Should provide management for controlling Power, Fan management, Chassis and compute node initialization, Switch management, Resource discovery and inventory management, Resource alerts and monitoring management, Chassis and compute node power management and diagnostics for elements including Chassis, I/O options and compute nodes. • Should Support the BIOS update even if the Server is Switched Off • Operating system failure window (blue screen) capture and display through the web interface • Syslog alerting mechanism that provides an alternative to email and SNMP traps • Secured security Policy with complex password policies for user and Mandatory change of password for all user accounts at first login • Should Support SSL, SSH, Https based access only for secured communication • Should able to Backup the current configuration and also can be able to restore previous configuration • There should be status indicator in console as Red or Green or Orange to check the health of the component • Should able to generate reports on the hardware activity changes. • Should show real time power consumption in the compute nodes	

S. No.	Features	Specifications Required	Compliance Code
11	System Panel	LEDs on the front information panel that can be used to obtain the status of the chassis Identify, Check log and the Fault LED	
12	Support for Multiple Platform	Should provide support for multiple platforms in x86 and RISC Blade servers within the same enclosure.	
13	Warranty	3 year onsite warranty with 24x7 The support should be directly from OEM	

5.5 SAN Storage

S. No.	Functionality	Compliance code
1.	The storage array should support industry-leading Operating System platforms including: Windows 2003, *Windows Server 2008, Windows Server 2012 or latest),* HP Tru64 UNIX, OpenVMS, Sun Solaris, HP-UX, IBM-AIX, Linux, non-stop OS and Mainframe.	
2.	The storage array should support multiple clusters of various operating systems mentioned above.	
3.	The storage array should be based on end to end minimum of 6Gbps technology and should have no single point of failure. In case, vendors can't provide the same then they shall ensure that at-least front-end ports are running at 8Gbps speed and back-end is running at 4Gbps.	
4.	The Storage Array should have a bladed switched architecture with separate front end boards (configured in pairs) and separate backend boards (configured in pairs).	
5.	Offered Array shall be scalable to minimum of 100TB capacity using 300GB SAS / FC drives.	
6.	It should be quoted with 2TB usable space for four clusters, with fault tolerance features. Total disk supported in the storage system should be at least 100 nos.	
7.	Drive Interface- 6Gb SAS disk ports. Should also support cheaper SATA or equivalent options with intermixing support. Supported Drives should be 300GB ,600GB and higher	
8.	There shall be no single point of failure into the array system including Power Supplies, Cache, Cache boards, Front-end Boards, Backend Boards etc.	
9.	The storage array should be based on an internal cross bar architecture or switched architecture.	
10.	Should have 8 numbers of 8 GB Fiber Channel host port and 16 X SAN Lane drive interface.	

S. No.	Functionality	Compliance code
11.	Storage subsystem shall be offered with encryption facility for actual data which is going to reside on the storage. Encryption for actual data shall be managed within the storage array instead of using any encryption software at switch or server environment.	
12.	Storage Array shall support RAID 1/10, 5/50, 6/60	
13.	Storage Array shall support both Spanning and Striping of volume across minimum of 32 channels.	
14.	RAID Controller Dual Active with 12 Cache (read/write/control) per RAID Controller	
15.	Cache should be mirrored and battery backed up to provide protection of data for more than 70 hours or shall have de-staging feature	
16.	Storage array shall be configured with at-least 2 global hot spare drives and drives shall be applicable to entire array than disk shelves.	
17.	The Storage solution should be architected to provide with 100 percent redundancy in the end to end solution	
18.	The Storage system should be configured with GUI-based Storage Management Software Tools for Management. A single command console should be used for the entire storage system	
19.	Must include Storage Manager software to centrally manage all disk storage subsystems, Multi path (Load Balancing & Failover) for minimum 8 hosts., LUN masking software for 8 hosts, Should support raid level migration	
20.	Storage system should support at least 3 Point in Time copies within the same storage system for a given production volume.	
21.	Storage system should have a support of virtualization engine which can allow consolidation of third party fabric based storage system as a Single array without using any client software or dedicated appliance for Production systems.	
22.	Storage subsystem shall allow creation of hardware or Firmware based business copies on third party fabric based storage system without loading any client software or dedicated appliance for production systems. Business copies shall support both full copy and incremental operations.	
23.	Storage should support 115000 or more IOPS&shalll be certified by OEM.	
24.	The storage system shall provide thin provisioning support which allows creating the volumes of bigger size than available capacity.	
25.	The storage system shall provide intelligent data tiering support so that on the basis of defined policies, only the selective data can be moved from a given Logical unit / Tier to another Tier.	

S. No.	Functionality	Compliance code
26.	The storage system should support non-disruptive component repair and hot replacement of Interfaces, Disk Controllers, Disk Drives, Cache memory cards, Power Supplies & Battery systems, Fan subsystems, Micro-code	
27.	The storage system should support automatic detection of errors, error logging and notification.	
28.	The storage system should support Pro-active maintenance – self monitoring, self diagnosing and wherever possible, self repairing features	
29.	The storage system should support data replication from One storage system to another storage system without any server intervention	
30.	The Storage system should be configured with HBA Load Balancing & Auto Failover software.	
31.	The Storage system should have storage management utilities that help in administering the storage. A single storage management console should be used for all storage management related activities. It should support the following: A centralized extensive monitoring, configuration and management of storage components and its connectivity components via a single console.	
32.	Ability to monitor the status, performance and configuration with utilization.	
33.	Ability to collect, store and analyze storage performance data.	
34.	Should have the flexibility to allow the users to set up, enable, delete and remove remote copy volumes, repairs and internal hardware copy volumes.	
35.	Others- All required cable and connectors to be supplied	
36.	Storage array should be supplied with 2 Nos of SAN switch with 8 Gbps FC* 16 Ports each	

5.6 Tape Library

S. No.	Features	Specifications Required	Compliance Code
1	Architecture	Offered Tape Library shall be Modular design to allow configuration, add capacity and increase performance as per requirement..	
2	Capacity & Scalability	1. The native LTO-5 capacity should be 1.5TB. 2. Shall be offered with Minimum of Two LTO5 tape drive in tape Library.	

S. No.	Features	Specifications Required	Compliance Code
3	Tape Drive Architecture	1. Offered LTO5 drive in the Library shall conform to the Continuous and Data rate matching technique for higher reliability. 2. Offered LTO5 drive should be hot swapable and shall support WORM and AES 256 bit encryption.	
4	Speed	Offered LTO5 drive shall support 140MB/sec in Native mode and 280MB/sec in 2:1 Compressed mode.	
5	Connectivity	Offered Tape drive shall provide FC native connectivity.	
6	Partitioning	1. Tape Library shall support Partitioning for the mixed media usage. 2. Partitioning shall be native feature to tape library and shall be done without using any external device.	
7	Management	1. Tape Library shall provide web based secure remote based management so that Tape Drives and robots can be assigned to clients on requests / Demand. 2. Tape Library shall have a mechanism to hold Persistent history and intelligent analysis of events and logs for easy troubleshooting.	
8	Cartridge Slots	1. Tape Library shall be offered with Minimum of 10 slots	
9	Other Features	1. Tape Library shall have GUI Panel 2. Shall be rack mountable. 3. Shall provide Redundant Power supply and cooling FANs. 4. Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action. 5. Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved.	

5.7 Internet Router

S. No.	Functionality	Compliance code
	General specification	
1.	All routers should beIPv4, IPv6 enabled and ready from Day-1. All the hardware & software licenses should be provided with the system.	
	Architecture	
2.	The router should be modular chassis and 19" rack mountable	
3.	Router shall have advanced Multi-Service Architecture delivering enhanced, integrated data, voice and security services	
4.	The router shall have two dual-personality Gigabit Ethernet ports, 10/100/1000BASE-TX (RJ-45) or SFP	
5.	The router shall have four WAN Interface card slots	
6.	The router shall have 4 x 10/100 Mbps WAN port	
7.	The router shall have Three free Network Module slots (wide slots) for further up gradation of WAN interfaces.	
8.	The router shall support LAN/WAN/Voice interface cards	
9.	The router shall have Hardware-based encryption acceleration	
10.	The router performance shall be minimum 800 Kpps	
11.	The router shall support VPN acceleration of 150 Mbps which can be upgraded to 600 Mbps	
12.	The router shall support Up to 3000 IPSec VPN Tunnels	
13.	The router shall be configured with minimum 256MB Compact Flash and 256MB SDRAM upgradeable to 1GB	
14.	The router shall have Built-in flash and USB slots that hold multiple configuration files and operating systems for recovery purposes	
15.	The router shall have internal redundant power supply	
	Features Supported	
16.	The router shall support IPv4 and IPv6 from day 1.	
17.	The router shall support the following WAN Protocols - HDLC, PPP, MLPPP, Frame Relay, MLFR, PPPoE, X.25, ISDN	
18.	The router shall support the following IP Routing Protocols (IPv4/IPv6) - RIP v1 and v2, OSPF, OSPF v3, BGP 4, BGP 4+, IS-IS, IS-ISv6	
19.	The router shall support non-IP protocols like IPX, SNA	
20.	The router shall support the following Interface Modules –ISDN PRI, E1/CE1, V.35 Serial, Ethernet, FXS, FXO, G.SHDSL, E3, STM1	
21.	The router shall support MPLS features like LDP, LSPM, MPLS TE, RSVP TE, MPLS FW, L2 MPLS, L3 MPLS form day-1.	
22.	The router firmware shall have security features such as advanced firewall, ACLs, L2TP, SSL, IPSec and MPLS VPNs	

S. No.	Functionality	Compliance code
23.	The router shall supports DES, 3DES, and AES 128/192/256 encryption, and MD5 and SHA-1 authentication	
24.	Firewall throughput of up to 1.5 G1bps	
25.	The router shall support multicast features including IGMP, PIM-SM, PIM-DM, PIM-SSM, MBGP, MSDP	
26.	The router shall support Policy-based routing (unicast/multicast)	
27.	Reliability features like VRRP	
28.	The router shall support common industry voice protocols including Session Initiation Protocol (SIP) and H.323	
29.	The router shall support IP Telephony module to deliver call processing capabilities	
30.	The router shall support QoS features including WFQ, CBQ, WRED, Low latency Queuing(LLQ), PQ, cRTP, MPLS QOS, Flow-based QoS policy	
31.	The router shall support NAT (Network Address Translation) & Port Address translation (PAT), SSH v1.5 and v2, uRPF, GRE	
32.	The router shall support central management through SNMP v1, v2c, v3, RMON	
33.	The router shall provide NetStream packet statistics or equivalent	
34.	The router shall support Web-based management, CLI, Telnet	
	Warranty and Support	
35.	Three Years warranty from OEM	

5.8 MPLS Router

S. No.	Functionality	Compliance code
	General specification	
1.	All routers should beIPv4, IPv6 enabled and ready from Day-1. All the hardware & software licenses should be provided with the system.	
	Architecture	
2.	The router should be modular chassis and 19" rack mountable	
3.	Router shall have advanced Multi-Service Architecture delivering enhanced, integrated data, voice and security services	
4.	The router shall have two dual-personality Gigabit Ethernet ports, 10/100/1000BASE-TX (RJ-45) or SFP	
5.	The router shall have four WAN Interface card slots	
6.	The router shall have 4 x 10/100 Mbps WAN port	
7.	The router shall have 4 x V.35 WAN Serial Interface.	
8.	The router shall have two free Network Module slots (wide slots)	

S. No.	Functionality	Compliance code
	for further upgradation of WAN interfaces.	
9.	The router shall support LAN/WAN/Voice interface cards	
10	The router shall have Hardware-based encryption acceleration	
11	The router performance shall be minimum 800 Kpps	
12	The router shall support VPN acceleration of 150 Mbps which can be upgraded to 600 Mbps	
13	The router shall support Up to 3000 IPSec VPN Tunnels	
14	The router shall be configured with minimum 256MB Compact Flash and 256MB SDRAM upgradeable to 1GB	
15	The router shall have Built-in flash and USB slots that hold multiple configuration files and operating systems for recovery purposes	
16	The router shall have internal redundant power supply	
	Features Supported	
17	The router shall support IPv4 and IPv6 from day 1.	
18	The router shall support the following WAN Protocols - HDLC, PPP, MLPPP, Frame Relay, MLFR, PPPoE, X.25, ISDN	
19	The router shall support the following IP Routing Protocols (IPv4/IPv6) - RIP v1 and v2, OSPF, OSPF v3, BGP 4, BGP 4+, IS-IS, IS-ISv6	
20	The router shall support non-IP protocols like IPX, SNA	
21	The router shall support the following Interface Modules –ISDN PRI, E1/CE1, V.35 Serial, Ethernet, FXS, FXO, G.SHDSL, E3, STM1	
22	The router shall support MPLS features like LDP, LSPM, MPLS TE, RSVP TE, MPLS FW, L2 MPLS, L3 MPLS form day-1.	
23	The router firmware shall have security features such as advanced firewall, ACLs, L2TP, SSL, IPSec and MPLS VPNs	
24	The router shall supports DES, 3DES, and AES 128/192/256 encryption, and MD5 and SHA-1 authentication	
25	Firewall throughput of up to 1.5 G1bps	
26	The router shall support multicast features including IGMP, PIM-SM, PIM-DM, PIM-SSM, MBGP, MSDP	
27	The router shall support Policy-based routing (unicast/multicast)	
28	Reliability features like VRRP	
29	The router shall support common industry voice protocols including Session Initiation Protocol (SIP) and H.323	
30	The router shall support IP Telephony module to deliver call processing capabilities	
31	The router shall support QoS features including WFQ, CBQ, WRED, Low latency Queuing(LLQ), PQ, cRTP, MPLS QOS, Flow-	

S. No.	Functionality	Compliance code
	based QoS policy	
32	The router shall support NAT (Network Address Translation) & Port Address translation (PAT), SSH v1.5 and v2, uRPF, GRE	
33	The router shall support central management through SNMP v1, v2c, v3, RMON	
34	The router shall provide NetStream packet statistics or equivalent	
35	The router shall support Web-based management, CLI, Telnet	
	Warranty and Support	
36	Three Years warranty from OEM	
	Management	
37	Shall have support for Web based management, CLI, Telnet and SNMPv3	
38	Shall support Secure Shell for secure connectivity.	
39	Shall support Out of band management through Console and external modem for remote management	

5.9 Branch Router

S. No.	Functionality	Compliance code
	General specification	
1.	All routers should beIPv4, IPv6 enabled and ready from Day-1. All the hardware & software licenses should be provided with the system.	
	Architecture	
2.	The router should be modular chassis and 19" rack mountable	
3.	Router shall have advanced Multi-Service Architecture delivering enhanced, integrated data, voice and security services	
4.	The router shall have two dual-personality Gigabit Ethernet ports, 10/100/1000BASE-TX (RJ-45) or SFP	
5.	The router shall have four WAN Interface card slots	
6.	The router shall have 3 x 10/100 Mbps WAN port	
7.	The router shall have 4 x V.35 WAN Serial Interface.	
8.	The router shall have two free Network Module slots (wide slots) for further upgradation of WAN interfaces.	
9.	The router shall support LAN/WAN/Voice interface cards	
10.	The router shall have Hardware-based encryption acceleration	
11.	The router performance shall be minimum 400 Kpps	
12.	The router shall support VPN acceleration of 100 Mbps	
13.	The router shall support Up to 250 IPSec VPN Tunnels	

S. No.	Functionality	Compliance code
14.	The router shall be configured with minimum 256MB Compact Flash and 256MB SDRAM	
15.	The router shall have Built-in flash and USB slots that hold multiple configuration files and operating systems for recovery purposes	
16.	The router shall have internal redundant power supply	
	Features Supported	
17.	The router shall support IPv4 and IPv6 from day 1.	
18.	The router shall support the following WAN Protocols - HDLC, PPP, MLPPP, Frame Relay, MLFR, PPPoE, X.25, ISDN	
19.	The router shall support the following IP Routing Protocols (IPv4/IPv6) - RIP v1 and v2, OSPF, OSPF v3, BGP 4, BGP 4+, IS-IS, IS-ISv6	
20.	The router shall support non-IP protocols like IPX, SNA	
21.	The router shall support the following Interface Modules –ISDN PRI, E1/CE1, V.35 Serial, Ethernet, FXS, FXO, G.SHDSL, E3, STM1	
22.	The router shall support MPLS features like LDP, LSPM, MPLS TE, RSVP TE, MPLS FW, L2 MPLS, L3 MPLS form day-1.	
23.	The router firmware shall have security features such as advanced firewall, ACLs, L2TP, SSL, IPSec and MPLS VPNs	
24.	The router shall supports DES, 3DES, and AES 128/192/256 encryption, and MD5 and SHA-1 authentication	
25.	The router shall support multicast features including IGMP, PIM-SM, PIM-DM, PIM-SSM, MBGP, MSDP	
26.	The router shall support Policy-based routing (unicast/multicast)	
27.	Reliability features like VRRP	
28.	The router shall support common industry voice protocols including Session Initiation Protocol (SIP) and H.323	
29.	The router shall support IP Telephony module to deliver call processing capabilities	
30.	The router shall support QoS features including WFQ, CBQ, WRED, Low latency Queuing(LLQ), PQ, cRTP, MPLS QOS, Flow-based QoS policy	
31.	The router shall support NAT (Network Address Translation) & Port Address translation (PAT), SSH v1.5 and v2, uRPF, GRE	
32.	The router shall support central management through SNMP v1, v2c, v3, RMON	
33.	The router shall provide NetStream packet statistics or equivalent	
34.	The router shall support Web-based management, CLI, Telnet	
	Warranty and Support	
35.	Three Years warranty from OEM	

5.10 Core Switch

S. No.	Functionality	Compliance code
	Architecture	
1.	Modular architecture, minimum six slots for interface modules	
2.	Shall have two dedicated switch fabric slots in addition to the interface modules	
3.	Shall have fully distributed architecture (any additional hardware required for the same shall be proposed)	
4.	Shall provide distributed Layer-2 (switching) and Layer-3 forwarding (Routing) on all line cards (any additional hardware required for the same shall be proposed)	
5.	Shall have minimum 700 Gbps of switching capacity	
6.	Shall have up to 350 Mpps of switching throughput	
7.	Shall support up to 200 Gigabit ports (Copper or SFP)	
8.	Shall support up to 20 10G ports (SFP+/XFP)	
9.	**Following are the ports requirement from Day 1:** i. 24 x 1G SFP ports ii. 48 x 10/100/1000 ports iii. x 10G SFP+ Ports iv. Shall have minimum one free slot for future expansion of ports	
10.	Shall be 19" Rack Mountable	
	Advanced Service Modules support	
11.	The switch shall support service modules to port applications directly to the switch chassis. This shall include support for the below service modules • Firewall and VPN module • Intrusion Prevention System (IPS) module • Wireless LAN services module • Server Load Balancer Module	
	Resiliency	
12.	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 router	
13.	Shall support virtual switching fabric creation across four chassis-based switches using 10G Ethernet Links	
14.	Hot-swappable Modules	
15.	Passive backplane with no active components for increased system reliability	
16.	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree	

S. No.	Functionality	Compliance code
	Protocol	
17.	IEEE 802.3ad Link Aggregation Control Protocol (LACP)	
18.	Ring protocol support to provide sub-100 ms recovery for ring Ethernet-based topology	
19.	Virtual Router Redundancy Protocol (VRRP) to allow a group of routers to dynamically back each other up to create highly available routed environments	
20.	Graceful restart for OSPF, IS-IS and BGP protocols	
21.	Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS and BGP protocols	
	Layer 2 Features	
22.	Shall support up to 4,000 port or IEEE 802.1Q-based VLANs	
23.	Shall support GARPVLAN Registration Protocol or equivalent feature to allow automatic learning and dynamic assignment of VLANs	
24.	Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops	
25.	Shall support IEEE 802.1ad QinQ and Selective QinQ to increase the scalability of an Ethernet network by providing a hierarchical structure	
26.	Shall support Jumbo frames on GbE and 10-GbE ports	
27.	Internet Group Management Protocol (IGMP)	
28.	Multicast Listener Discovery (MLD) snooping	
29.	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
30.	Multicast VLAN to allow multiple VLANs to receive the same IPv4 or IPv6 multicast traffic	
	Layer 3 Features (any additional licenses required shall be included)	
31.	Static Routing for IPv4 and IPv6	
32.	RIP for IPv4 (RIPv1/v2) and IPv6 (RIPng)	
33.	OSPF for IPv4 (OSPFv2) and IPv6 (OSPFv3)	
34.	IS-IS for IPv4 and IPv6 (IS-ISv6)	
35.	Border Gateway Protocol 4 with support for IPv6 addressing	
36.	Policy-based routing	
37.	Unicast Reverse Path Forwarding (uRPF)	
38.	IPv6 tunneling to allow IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet	
39.	Dynamic Host Configuration Protocol (DHCP) client, Relay and	

S. No.	Functionality	Compliance code
	server	
40.	PIM Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Source-Specific Mode (PIM-SSM) for IPv4 and IPv6 multicast applications	
	QoS and Security Features	
41.	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network	
42.	Port-based rate limiting and access control list (ACL) based rate limiting	
43.	Congestion avoidance using Weighted Random Early Detection (WRED)	
44.	Powerful QoS feature supporting strict priority (SP) queuing, weighted round robin (WRR) and weighted fair queuing (WFQ)	
45.	IEEE 802.1x to provide port-based user authentication with multiple 802.1x authentication sessions per port	
46.	Media access control (MAC) authentication to provide simple authentication based on a user's MAC address	
47.	Dynamic Host Configuration Protocol (DHCP) snooping to prevent unauthorized DHCP servers	
48.	Port security and port isolation	
	Management Features	
49.	Configuration through the CLI, console, Telnet, SSH and Web Management	
50.	SNMPv1, v2, and v3 and Remote monitoring (RMON) support	
51.	sFlow (RFC 3176) or equivalent for traffic analysis	
52.	Management security through multiple privilege levels with password protection	
53.	FTP, TFTP, and SFTP support	
54.	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port. Shall support minimum four mirroring groups	
55.	RADIUS/TACACS+ for switch security access administration	
56.	Network Time Protocol (NTP) or equivalent support	
57.	Shall have Ethernet OAM (IEEE 802.3ah) management capability	
	Environmental Features	
58.	Shall provide support for RoHS and WEEE regulations	
59.	Shall be capable of supporting both AC and DC Power inputs	
60.	Operating temperature of 0°C to 45°C	
61.	Safety and Emission standards including UL 60950-1; IEC 60950-1; VCCI Class A; EN 55022 Class A	
	Warranty and Support	
62.	The below Warranty shall be offered directly from the switch OEM Three Years Warranty with advance replacement	

5.11 Access Switch-24 Ports

S. No.	Functionality	Compliance code
Architecture		
1.	The switch should have 24 x 10/100/1000BaseT ports with 4 x 1000 Base-SXSFP ports. 1 x 1000 Base-LX to be supplied with LC type connector	
2.	Should support 1000 Base-SX, LX, BX, LH and 100Base-FX Mini-GBICs	
3.	The Switch should be 19" Rack-Mountable	
4.	Min. 48 Gbps switching capacity	
5.	MAC Address table size of 8,000 entries	
6.	All the switch ports should offer non-blocking, wire speed performance	
7.	Should support stacking of switches	
Resiliency and high availability		
8.	Should have internal/external redundant power supplies	
9.	Should support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk	
10.	Should support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP	
11.	Should support RADIUS VLAN for voice using standard RADIUS attribute and LLDP-MED to automatically configure VLAN for IP phones	
Layer 2 Switching		
12.	Should support IEEE 802.1Q VLANs,	
13.	Should support GARPVLAN Registration Protocol (GVRP) allowing automatic learning and dynamic assignment of VLANs	
Security Features		
14.	Should support protected ports to isolate specified ports from all other ports on the switch	
15.	Should support Port security, MAC Lockdown and MAC lockout	
16.	Should support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in conjunction with a RADIUS server	
17.	Should support Web-based authentication to authenticate clients that do not support the IEEE 802.1X supplicant	
18.	Should support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address	
19.	Should support BPDU port protection preventing forged BPDU attacks	
20.	Should support management access (CLI, Web, MIB) securely	

S. No.	Functionality	Compliance code
	encrypted through SSHv2, SSL, and SNMPv3	
Convergence and QoS		
19	Should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
20	Should support IEEE 802.1p Traffic prioritization delivering data to devices based on the priority and type of traffic	
Management Features		
21	Should support SNMPv1/v2c/v3	
22	Should support RMON providing advanced monitoring and reporting capabilities for statistics, history, alarms, and events	
23	Should support Full-featured command-line interface (CLI) and Web Interface for switch configuration	

5.12 Access Switch-48 Ports

S. No.	Functionality	Compliance code
Architecture		
1.	The switch should have 48 x 10/100/1000BaseT ports with 4 x 1000 Base-SXSFP ports. 1 x 1000 Base-LX to be supplied with LC type connector	
2.	Should support 1000 Base-SX, LX, BX, LH and 100Base-FX Mini-GBICs	
3.	The Switch should be 19” Rack-Mountable	
4.	Min. 96 Gbps switching capacity	
5.	MAC Address table size of 8,000 entries	
6.	All the switch ports should offer non-blocking, wirespeed performance	
7.	Should support stacking of switches	
Resiliency and high availability		
8.	Should have internal/external redundant power supplies	
9.	Should support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk	
10	Should support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP	
11	Should support RADIUS VLAN for voice using standard RADIUS attribute and LLDP-MED to automatically configure VLAN for IP phones	
Layer 2 Switching		
12	Should support IEEE 802.1Q VLANs,	
13	Should support GARPVLAN Registration Protocol (GVRP) allowing	

S. No.	Functionality	Compliance code
	automatic learning and dynamic assignment of VLANs	
Security Features		
14	Should support protected ports to isolate specified ports from all other ports on the switch	
15	Should support Port security, MAC Lockdown and MAC lockout	
16	Should support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in conjunction with a RADIUS server	
17	Should support Web-based authentication to authenticate clients that do not support the IEEE 802.1X supplicant	
18	Should support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address	
19	Should support BPDU port protection preventing forged BPDU attacks	
20	Should support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, and SNMPv3	
Convergence and QoS		
21	Should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
22	Should support IEEE 802.1p Traffic prioritization delivering data to devices based on the priority and type of traffic	
Management Features		
23	Should support SNMPv1/v2c/v3	
24	Should support RMON providing advanced monitoring and reporting capabilities for statistics, history, alarms, and events	
25	Should support Full-featured command-line interface (CLI) and Web Interface for switch configuration	

5.13 Access Switch POE

S. No.	Functionality	Compliance code
Architecture		
1.	The switch should have 24 x 10/100/1000BaseT ports with 4 x 1000 Base-SXSFP ports. 1 x 1000 Base-LX to be supplied with LC type connector , PoE support from day 1	
2.	Should support 1000 Base-SX, LX, BX, LH and 100Base-FX Mini-GBICs	
3.	The Switch should be 19" Rack-Mountable	
4.	Min. 48 Gbps switching capacity	

S. No.	Functionality	Compliance code
5.	MAC Address table size of 8,000 entries	
6.	All the switch ports should offer non-blocking, wirespeed performance	
7.	Should support stacking of switches	
Resiliency and high availability		
8.	Should have internal/external redundant power supplies	
9.	Should support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk	
10	Should support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP	
11	Should support RADIUS VLAN for voice using standard RADIUS attribute and LLDP-MED to automatically configure VLAN for IP phones	
Layer 2 Switching		
12	Should support IEEE 802.1Q VLANs,	
13	Should support GARPVLAN Registration Protocol (GVRP) allowing automatic learning and dynamic assignment of VLANs	
Security Features		
14	Should support protected ports to isolate specified ports from all other ports on the switch	
15	Should support Port security, MAC Lockdown and MAC lockout	
16	Should support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in junction with a RADIUS server	
17	Should support Web-based authentication to authenticate clients that do not support the IEEE 802.1X supplicant	
18	Should support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address	
19	Should support BPDU port protection preventing forged BPDU attacks	
20	Should support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, and SNMPv3	
Convergence and QoS		
21	Should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
22	Should support IEEE 802.1p Traffic prioritization delivering data to devices based on the priority and type of traffic	
Management Features		
23	Should support SNMPv1/v2c/v3	
24	Should support RMON providing advanced monitoring and reporting capabilities for statistics, history, alarms, and events	
25	Should support Full-featured command-line interface CLI) and	

S. No.	Functionality	Compliance code
	Web Interface for switch configuration	

5.14 UTM

S. No.	Features	Specifications Required	Compliance Code
1.	Support		
2.		Firewall & Integrated IPSEC VPN Applications should be EAL4 / FIPS 140-2 / ICSA certified	
		The hardware platform & firewall with integrated IPSEC VPN application has to be from the same OEM.	
		The Firewall should have remote access features like IPSec Client to Site VPN	
		Appliance should support for high availability deployment in Active – Active mode. It should not depend upon any 3rd party product or appliance for the same.	
		It should support the protection of unlimited IP hosts	
		Firewall Architecture should be on multiple tiers (firewall module, logging & policy management server, and the GUI/WebUI Console)	
		The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted	
		Firewall should support for static and dynamic routing capabilities. The firewall should support open standard protocols like RIP, OSPF and BGP	
		Firewall system should have support to configure QoS for the network traffic	
		The firewall should have at least local hard-disk or equivalent, in order to keep the event logs in the event of management server connection failure, etc. Provide detailed information	
3.	Interface and Connectivity Requirements	The firewall must be supplied with at least 8 10/100/1000Mbps interfaces on Copper.	
		The platform should support VLAN tagging (IEEE 802.1q) .	

S. No.	Features	Specifications Required	Compliance Code
		Firewall should support Active/Active with Stateful Failover for IPSec VPN Connections.	
		Firewall should have a dedicated Console port	
		Firewall should have a Management port	
		Should be IPv6 Compliant	
4.	Performance Requirements	The Firewall should support throughputs of minimum 4 Gbps for Clear text traffic	
		Provide information on the concurrent sessions supported Should support 1000,000 concurrent sessions. Should provide minimum 50,000 New Session per second	
		IPS Througput 1 Gbps	
		Provide information on the IPSEC VPN throughput supported Should provide minimum 500 Mbps of 3DES/AES256 encryption	
5.	Firewall Filtering Requirements	The Firewall should also support the standard Layer 3 mode of configuration with Interface IP's. It should be possible to protect the firewall policies from being compromised.	
		The Firewall must provide state engine support for all common protocols of the TCP/IP stack	
		The Firewall must provide NAT functionality, including dynamic and static NAT translations	
		The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type and time	
		The Firewall should be able to filter traffic even if the packets are fragmented.	
		All internet based applications should be supported for filtering like Telnet, FTP, SMTP, HTTP, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, MS-Exchange etc	
		It should support the VOIP Applications Security by supporting to filter SIP, H.323, &MGCP flows.	
		The Firewall should support authentication protocols and have support for firewall passwords, smart cards, & token-based products, and X.509 digital certificates.	
		The Firewall should support database related filtering and should have support for Oracle,	

S. No.	Features	Specifications Required	Compliance Code
		MS-SQL, and Oracle SQL-Net.	
		The Firewall should provide advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications	
		Support for Filtering TCP based applications	
		Support basic inspection HTTP, FTP & SMTP traffic	
		Should support CLI & GUI based access to the firewall modules	
		Local access to firewall modules should support role based access	
		Local access to the firewall modules should support authentication protocols – RADIUS / TACACS+	
		The firewall should be capable of carrying out the QoS functionality like allocation of bandwidth to applications	
6.	Firewall/IPSec VPN Management Server requirements	Firewall Real-Time Monitoring, Management & Log Collection (with storage) and Systems Resource Monitoring should be provided in the Centralized Management.	
		Firewall policies can be enforced from centralized management server at DC.	
		Firewall Management Systems should support High Availability and support the automatic replication & synchronization of the security policies and objects.	
		Any changes or commands issued by an authenticated user should be logged	
		Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter.	
		Real Time Monitoring, Appliance Health Monitoring, Security Policy Rollout for Firewall Systems on the Firewall appliances and Logs Collection from the Firewall appliances should be from single Management Server/Appliance	
		The Firewall Management system should only support communication to well defined system and all the communication should be	

S. No.	Features	Specifications Required	Compliance Code
		encrypted.	
7.		The UTM functionality should include URL Filtering and Antivirus Scanning with 200 Mbps throughput.	

5.15 Wireless Access Points

S. No.	Functionality	Compliance code
1.	The proposed architecture should be based on centralized controller with thin AP deployment. AP's should download OS and configuration from controller. Switch/Controller for improved security.	
2.	The controller should be capable of supporting 64 AP's from day 1 with the offered controller without any addition of Hardware components. Controller should have 25 AP license from day 1.	
3.	All the products (Controllers, thin APs, and remote APs) should run the same software and operating system for easier management and future upgradeability.	
4.	The controller should have minimum of 4 x 1GE port for connecting to LAN.	
5.	Redundancy Features: Active: Standby; Active: Active and 1: Many redundancies. Licenses of each Wireless switch/Controller should be aggregated so that all the licenses are usable.	
6.	The controller should support 802.11ac standard.	
7.	The controllers will be implemented in HA mode. When the primary controller fails and secondary controller comes up, the clients connected at point in time and all applications running on the clients should not disconnect.	
8.	Solution should provide differentiated access for Guests and staff group on same SSID, guests should have restricted access like not able to telnet &SSH to servers while connecting on same SSID. Same SSID should provide full access to senior diplomats and ministers.	
9.	The system should enable single session for Guest Wireless Access implying to disable multiple authentications using same user account	
10	Ministers/Diplomats and staff should be able to connect to wireless network once and be able to get different SLA or QoS for different applications.	
11	The system should provide different type of bandwidth cap for different groups like 2 MBPS for staff and 4 Mbps to	

S. No.	Functionality	Compliance code
	Ministers/Diplomats on same SSID.	
12	As per PCI compliance guidelines and access layer security there should be firewall (Integrated or overlay) segregation between Core switch and WLAN clients connected. Complete traffic has to be inspect deeply before reaching core switch if coming from access point.	
13	Rules for access rights should be based on any combination of time, location, user identity and device identity.	
14	The controller should be capable of dynamic Channel allocation to AP. The controller should have the capability to monitor interference and respond by allocating least or non-interfering channel to the AP's automatically. No manual intervention should be required.	
15	WLAN users normally use ping to check connectivity and this creates huge traffic in case of large no of users. WLAN should prevent users to use configured ping/icmp session windows which will also help to prevent these type of common DoS attacks	
16	As video & voice applications in Staff/Ministers/Diplomats smart devices/systems are vulnerable to delay & jitter, WLAN system should be capable enough to detect them to provide high priority on basis of application, device and user. System should dynamically defer off-channel scanning upon detection of voice and video traffic from device.	
17	WLAN system should allow unauthenticated staff or guests to allow navigate to ministry webpage & all its contents (not just homepage).	
18	The controller should provide latest network authentication (WEP, WPA, WPA2) and encryption types like DES/3DES, TKIP and AES.	
19	In addition to serving clients, controller should perform spectrum analysis to detect and classify sources of interferences. System should provide fast Fourier transform displays and spectrograms for real-time troubleshooting and visualization. This can be inbuilt in controller or add-on component can be provided to achieve it.	

Indoor Access Points Specifications

S. No.	Functionality	Compliance code
1.	IEEE 802.11n, min 3 x 3 MIMO, 3 spatial streams capable of 450 Mbps per radio. Dual Radio capable of being configured in 2.4 and 5 Ghz . 2x10/100/1000 Ge , GE POE built-in port	
2.	802.11 a/b/g/n functionality certified by the Wi-Fi alliance	

S. No.	Functionality	Compliance code
3.	Access Point can have integrated or external Antenna.	
4.	The min transmit power of AP should be 23dbm for both 2.4 and 5 ghz radio however Max transit power of the AP + Antenna should be as per WPC norms for indoor Access Points. OEM to give a undertaking letter stating that the AP will configured as per WPC guidelines for indoor AP and also submit the WPC certificate showing approval.	
5.	Transmit power of AP's should be in incemental of 1 db/as per regulatory domain	
6.	AP mounting kit should be with locking mechanism so that AP cannot be removed without using special tools.	
7.	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.	
8.	Should support BPSK, QPSK, 16-QAM and 64-QAM modulation types	
9.	Association rate from 1Mbps-54Mbps for b/g/a and MCS0 - MSC15 for 802.11n	
10	Should be UL2043 certified	
11	All AP's should supplied with POE injectors	

5.16 UTP System

S. No.	Features	Specifications Required	Compliance Code
UTP Cabling System			
1.	Type	Unshielded twisted pair cabling system, TIA / EIA 568-B.1 addendum Category 6 Cabling system	
2.	Networks Supported	10 / 100 Ethernet, 155 Mbps ATM, 1000 Mbps IEEE 802.3ab Ethernet, and proposed Cat 6 Gigabit Ethernet	
3.	Standards		
4.	TIA / EIA 568-B.1	ETL Verified	
5.	Warranty	Warranty to cover the performance of the specified and installed cabling system.	
6.	Performance Characteristics to be provided	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4-Connector channel	
UTP Cable			
7.	**Type**	**UTP, Category 6 Cabling system**	

S. No.	Features	Specifications Required	Compliance Code
8.	Material		
9.	Conductors	24 AWG solid bare copper	
10.	Insulation	Polyethylene	
11.	Separator	Should be a cross filler. Any other filler type, like bi-directional	
12.		Strip would not be acceptable.	
13.	Jacket	Flame Retardant PVC	
14.	Approvals	UL Listed	
15.		ETL verified to TIA / EIA Cat 6	
16.	Operating Temperature	-20 Deg. C to +60 Deg. C	
UTP Jacks			
17.	**Type**	**PCB based, Unshielded Twisted Pair, Category 6,TIA / EIA 568-B.2**	
18.	Durability		
19.	Modular Jack	750 mating cycles	
20.	Wiring blocks	Polycarbonate, 94V-0 rated	
21.	Jack contacts	Phosphorous bronze, plated with 1.27micro-meter thick gold	
22.	Approvals	UL listed	
UTP Jack Panels			
23.	Type	24-port, Modular, PCB based, Unshielded Twisted	
		Pair, Category 6, TIA / EIA 568-B.2	
24.	Ports	24 Port	
25.	Category	Category 6	
26.	Identification Scheme	Icons on each of 24-ports	
27.	Port Identification	9mm or 12mm Labels on each of 24-ports (to be included in supply)	
28.	Height	1 U (1.75 inches)	
29.	Modular Jack	750 mating cycles	
30.	Jack details	Same as above	

5.17 Patch Cords

S. No.	Features	Specifications Required	Compliance Code
1.	Type	Unshielded twisted pair cabling system, TIA / EIA 568-B.1 addendum Category 6 Cabling system	

S. No.	Features	Specifications Required	Compliance Code
2.	Conductor	24 AWG 7 / 32, stranded copper	
3.	Length	7-feet for workstation and 3-feet for Jack panel/equipment	
4.	Plug Protection	Matching colored snag-less, elastomer polyolefin boot	
5.	Warranty	25-year component warranty	
6.	Category	Category 6	
7.	Plug		
8.	Housing	Clear polycarbonate	
9.	Terminals	Phosphor Bronze, 50 micron gold plating over selected area and gold flash over remainder, over 100 micron nickel under plate	
10.	Load bar	PBT polyester	
11.	Jacket	PVC	
12.	Insulation	Flame Retardant Polyethylene	

5.18 PC-Desktop

S. No.	Features	Specifications Required	Compliance Code
1.	Processor:	Core i7 3770 (3.40 GHz, 8MB L3 cache)	
2.	Motherboard	Intel 7 series chipset based OEM motherboard with support for PCI Express x16 graphics port. Motherboard should be ROHS compliant.	
3.	BIOS	With support for: Flash, Plug and Play, DMI 2.0, ACPI	
4.	Memory:	4 GB / 8 GB DDRIII RAM Memory @ 1333/1600 MHz or better with 2 DIMM slots Expandable upto 16 GB	
5.	Hard Disk Drive:	500 GB 7200 rpm SATAII (3Gb/s) Drive with pre-failure alert with 8MB Cache Buffer	
6.	Hard Disk Controller:	Integrated On-Board Hard Disk Controller supporting Serial ATA Interfaces	
7.	Monitor	18.5" Wide TFTTCO 05 monitor. Monitor resolution to be 1366*768. Aspect ratio of 16:9, response time: 5 ms, contrast ratio: 1000:1. Windows 8–certified touch-screen monitor	
8.	Key Board	104 Keys or more Multimedia Keyboard Rupee ready isolated keyboard	
9.	Mouse	USB/PS2 Optical Scroll Mouse	

S. No.	Features	Specifications Required	Compliance Code
10.	Network Card	Integrated on board Ethernet Controller 10/100/1000 with PXE support and Remote wake up, Wireless LAN:802.11b/g/n	
11.	Interfaces	1Serial, 1 parallel, Minimum 6 USB Ver. 2.0 (with 2 in front). 1 USB 3.0 port, & Audio Ports	
12.	Expansion-Graphics Slots	4 PCI series slots including minimum 1 PCI E X16 slot and atleast 1 PCI slot	
13.	Cabinet	MATX Cabinet with atleast 4 bays (2x5.25" External, 1x3.5" External, 1x3.5" Internal)	
14.	Audio	Integrated on board ALC 892 or higher Audio Controller	
15.	Power Supply	200 W SMPS	
16.	Certifications AND Compliance's	ISO 9001: 2000 for OEM Manufacturing, Windows OS Certification, Microsoft certificate of authenticity – COA to have OEM's name, Direct Named OEM and Partner certificate from Intel	
17.	Other S/W Tools/Licenses	Single utility software for:	
		Application and data recovery	
		Secure data removal (permanent and irreversible)	
		Asset health and tracking software	
		A web based management console that provides a single interface to manage all the systems in a site	
18.	AV	MCAFEE WITH 3 YEARS SUBSCRIPTION	
19.	Operating System:	OEM Windows 8 Prof. with recovery media to be preloaded. Vendor must furnish a list of serial numbers of all CoA along with the corresponding list of PC system serial numbers for Operating system licenses which are pre-loaded	
20.	Application Software	MS Office 2013 Pro PRELOADED IN DESKTOP	
21.	CERTIFICATIONS AND OTHER QUALITY DOCUMENTS	GREEN PEACE RATING OF 5.0 AND ABOVE	
22.	Warranty	OEM warranty for three years	

5.19 Laptop

S. No.	Features	Specifications Required	Compliance Code
1.	Processor	Intel Core i5-3rd generation	
2.	Chipset	Intel 7 Series Chipset	
3.	System Memory	System Memory 4GB Upto 8GB supported, 1333MHz Dual Channel DDR3,2 DIMM slots	
4.	Graphics	Integrated HD Graphics	
5.	Hard Drive	Primary Storage Options 500 GB 5400 RPM SATA Hard Drive or higher	
6.	Optical Drive	Optical Drive 8X or above DVD+/-RW with double-layer DVD+/-R write capability	
7.	Display	Touch screen Display14" High Definition Wide LED Anti-Glare Display (1366x768)	
8.	Audio / Visual	Integrated stereo speakers Stereo headphone/lineout/ Two built-in stereo speakers High- definition audio support MS- Sound compatible, Built-in digital microphone	
9.	Communications	WIFI	
10.	Integrated Wireless	WirelessLAN:802.11b/g/n and Bluetooth®4.0+HS Bluetooth® 2.1+EDR	
11.	Keyboard	Keyboard 86-/87-/91-key Fine Tip keyboard with international language Media keys Control keys Wireless LAN key	
12.	Pointing Device	Support Touchpad, Multi- gesture touchpad, supporting two-finger scroll, pinch, rotate, flip	
13.	Battery	Battery Options 6-cell (48 WHr) Lithium Ion battery integrated with optional long lifecycle battery	
14.	Interfaces / Ports	Media Card Reader - One(1) VGA One(1)HDMI- One(1) Stereo microphone in -One(1) Stereo headphone/line out- One(1) Power connector - One(1) RJ-45/Ethernet -One(1) USB 2.0- 2 and USB (3.0) – 1	
15.	Operating System	Genuine Windows(R) 7 Professional SP1 (English) or above with updates / patches & MS Office 2013 Pro Pre Loaded	
16.	Drivers for Different Operating systems	Drivers should be freely available on OEM's website and should be supplied in media along with PC	

S. No.	Features	Specifications Required	Compliance Code
17.	Antivirus	latest ant virus with five year updation facility	
18.	Additional Requirement	Manufacturer should be listed in any quadrant of independent technology and market research companies such as Gartner and Forrester Research in last 3 years	

5.20 Multi-Functional Printer

S. No.	Features	Specifications Required	Compliance Code
1.	Type	Desktop	
2.	Printing processing Technology	Laser beam scanning & Electro photographic printing (Black)	
3.	Resolution (dpi, bit/pixel)	1200 x 1200 dpi	
4.	Printer Language	PCL 6, PostScript 3 emulation	
5.	Printing Speed	(A4) 28 pages per minute (A4) , 30 Pages Per Minute (LT)	
6.	First Print Speed	Less than 8 sec	
7.	Memory Standard :	128 MB	
8.	Duplex	Automatic	
9.	Duty Cycle	35000/ month	
10.	Dimensions (WxDxH)	Less than 420 x 397 x 442mm	
11.	Weight Less than	18 kg	
12.	Input capacity Std Tray	250 sheets (80 g/m2)	
13.	Bypass tray	50 sheets (80 g/m2)	
14.	Output capacity	Up to 125 sheets	
15.	Input Paper Size	A4,B5,A5,B6,A6,Legal,Letter,HLT,Exective, Folio	
16.	Media Type	Plain Paper, Recycle Paper, Bond Paper, Envelopes, Labels	
17.	Paper Weight	52-162 g/m2	
18.	ARDF Capacity	35 sheets	
19.	Interface	USB 2.0, 100 Base-Tx/10 Base - Tx Ethernet	

S. No.	Features	Specifications Required	Compliance Code
20.	Supported environments	Windows 2000/XP/Server 2003/Vista/Server 2008, Mac OS x 10.2.8 - 10.5	
21.	Rating Power Spec.	220-240V, 50/60Hz	
22.	Processor	400 Mhz	
23.	**Copier Features**		
24.	Copy Speed	(A4) 28 copies per minute (A4), 30 Pages Per Minute (LT)	
25.	Multiple copy	Up to 99	
26.	Resolution	1200 x 1200 dpi	
27.	Reduction / Enlargement	25 to 400%	
28.	Copy mode (Image quality mode)	Text / Photo / Mixed	
29.	**Fax Features**		
30.	Circuit	PSTN/ PBX	
31.	Compatibility	ITU-T G3	
32.	Coding System Compression Method	MH/MR/MMR	
33.	Fax modem speed	33.6 kbps	
34.	Transmission Speed	Approx. 3sec, Compression : MMR, Resolution : Standard speed: 33.6kbps	
35.	Memory capacity	100 pages (ITU No.1 chart, Compression : MMR, Resolution: Standard)	
36.	Memory Backup	1 hour	
37.	One Touch Dial	20 locations	
38.	Speed Dial/Group Dial	50 locations / No	
39.	PC FAX	Yes (Only transmission)	
40.	**Scanner Feature**		
41.	Scanning Device	CCD array image-sensor	
42.	Resolution Standard	1200 x 1200 dpi	

S. No.	Features	Specifications Required	Compliance Code
43.	Maximum	19200 x 19200 dpi (interpolated)	
44.	Gray scale	256 levels	
45.	Colour scan depth	48bit colour processing (input), 24bit colour processing (output)	
46.	Scan modes	ADF& Platen	
47.	TWAIN Compliant	TWAIN, WIA	
48.	Scan to e-mail	SMTP, TCP/IP	
49.	Scan to folder Via	SMB or FTP protocol	
50.	Scan to USB	YES	
51.	Scanner utilities & Drivers	TWAIN Driver, Scanner utility (PageManager)	

5.21 Biometric Device

S. No.	Specification Required	Compliance Code
	Technical Specifications:	
1	Sensor type: Optoelectronic	
2	Optical architecture : Dual prism, macro lens	
3	Platen area (effective) : 18mm x 26mm	
4	Glass thickness / type : 25mm/crown scratch resistant	
5	Resolution : 500 / 512 PPI	
6	Image grey scale : 256 level Dynamic	
7	Scanning time : 0.01Sec.	
8	Distortion rate : 0.1%	
9	Computer interface : USB2.0 , USB Powered	
10	Operating temperature : 0 – 55 Degree C	
11	Humidity : Up to 90%	
12	Optical coating : Hygroscopic	
	Salient Features:	
13	Enrollment /Transaction Grade	
14	Professional grade optics & sensor	
15	High Speed 2.0 USB Interface	
16	Fast scanning and live display of capture image	
17	Different attributes image levels with auto adjustment	
18	Non-distorted image quality	
19	No problem in capturing smeared, scarred, stained, smudged fingers , dry & wet fingers	

S. No.	Specification Required	Compliance Code
20	Heavy duty and long USB cable	
21	Industrial grade chassis for durability	
	Supported Operating Systems:	
22	MS Windows	
23	Linux	
	SDK/API Environment:	
24	C#.NET, VB.NET, VB 6.0, VC ++ 6.0	
25	Java- Application & applet	
	Standards Compliance:	
26	ISO/IEC 19794-4 Fingerprint Image Data Standard	
27	FIPS 201 PIV	
28	Compatible with all FP matching algorithms	
29	Should integrate with CCI Application	