

Guidelines for Infrastructure & Application Hosting in SDC

V 1.0

Department of Electronics & Information Technology,
Ministry of Communications and Information Technology,
Government of India

Abstract

This document is intended to assist the State Implementing Agencies and the user departments intending to host applications in the SDC while providing information about various services available from SDC, various application hosting models, stakeholders and their relationships etc.

Introduction

State Data Centre (SDC) is one of the key infrastructure pillars that is being set up at every State / UT to consolidate citizen services, eGovernance applications and supporting infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. These services shall be rendered by the States through a common delivery platform supported by other core infrastructure elements i.e. SWAN and CSC with connectivity extended up to the block level. The SDCs shall therefore enable aggregation of IT Infrastructure (Hardware, Storage, Networking and Software) and Management Resources to ensure better Operations, Standardization of Systems & management control leading to faster application deployment and reduced costs, offering dynamic scalability as their demand grows including security related requirements and uptime of the highest order. Thus, different line department would get a seamless, highly reliable/robust, shared, secured Data Centre infrastructure with reasonable/scalable capacity for their eGovernance application hosting requirements. SDC would provide better operations & management control and minimize overall cost of Data Management, IT Management, Deployment and other costs.

The intent of this document is to encourage User Departments at the State to host their infrastructure and application inside the State Data Centre as soon as they are ready and can be deployed in the production environment.

SDC Infrastructure

The State Data Centre would provide a secure and highly available physical infrastructure including rack space; UPS, Air Conditioning, DG sets, fire prevention, access control systems etc designed and implemented meeting at least Tier II data center guidelines with 99.749% availability. The core IT infrastructure for routing, switching, firewall security, storage, access control, authentication etc would provide a foundation infrastructure necessary for every application delivering services through web or intranet. Apart from the core IT infrastructure, compute infrastructure including database, application and web servers envisaged would enable the State to initially host a few applications and also in shared manner. Eventually the SDC would become centralized information/application warehouse for eGovernance in the State.

The State Data Centres (SDCs) would thus help the State Government and Departments in providing central repository (database consolidation), application consolidation, State Intranet/Internet portal, State messaging infrastructure, remote management, business continuity site etc. for their G2G, G2C service delivery and G2B services. State Data Centre would also help in providing common security infrastructure, storage infrastructure, back-up infrastructure, directory infrastructure, web servers, application servers, database servers etc. The SDC thus established would be able to meet various application hosting requirements. If the infrastructure is adequately scaled up, the SDC may take care of hosting requirements in the State for another 5 year period. A list of SDC components is enclosed at Annexure II for reference.

The scalability of infrastructure that have been provisioned under the SDC scheme for the States/UTs, is prepared keeping in mind the requirement for User departments, State Government and MMPs

applications and infrastructure that are expected to be hosted in SDC. Each MMP and State Department is required to contact the State Composite Team with details of the required shared infrastructure and services that can be leveraged from SDC to check the availability of the same.

Services available from SDC


There are various services which shall be available from SDC and can be leveraged on mutually agreed terms between the State Implementing Agency (SIA)/ Composite Team (CT), concerned line ministry/department and the Data Centre Operator (DCO). The services can be broadly categorized as:

Infrastructure Services: These would be mainly related to leveraging the physical & Core IT infrastructure and associated services by the line departments.


Managed Services: These would be mainly related to leveraging the O & M requirements in the SDC through Composite team/Data Centre Operator.

A logical overview of the services available under these is depicted below:

Infrastructure Services	Managed Services
Rack Space	Managed Security Services
Seating Space	Backup Services
Staging Facility	Vendor Management
Connectivity to SWAN & Internet	Basic Hardware and OS level Support
Facility Management	Storage Configuration & management
Shared Storage	Helpdesk Services
Shared Compute Infrastructure	Common IT Support Services
	Monitoring
	Disaster Recovery
	Directory Services



Components : HVAC, UPS, DG set, Storage, BMS, EMS, CCTV surveillance System etc



Components : Firewall, antivirus, storage management, backup, Servers, Databases etc

leverage the SWAN for connectivity purposes. Similarly high bandwidth common, secure, high available internet connectivity has been provisioned.

- v. **Facility Management:** The DCO shall provide Facility Management Services for the entire physical infrastructure present at the SDC. A building management system (BMS) has been procured for this purpose.
- vi. **Shared Storage:** A centralized storage with management and flexible, secure configuration shall be available. Depending upon the requirement of the department and as agreed with the SIA/Composite team, the same can be leveraged.
- vii. **Shared Compute Infrastructure :** To cater to the needs of application hosting at the State an initial compute infrastructure consisting of Application, Web and Database servers with different flavors of software/OS has been provisioned in the SDC which can be leveraged in shared manner to meet needs of several state eGovernance applications. The same may also be used for the application selected for the purpose of Final Acceptance Test (FAT) of SDC. Optimal utilization of these servers would be able to cater to the needs of multiple applications. Once these components reach the stage of full utilization, then the State will have to provision for additional procurement or the user departments might have to bring their own application and database servers.

Managed Services:

- i. **Managed Security Services:** The SDC shall be designed for an end-to-end security blanket to protect applications, services, data and the infrastructure from malicious attacks or theft from external & as well as Internal hackers. The various components provisioned under the SDC scheme to meet this objective are:
 - Firewall
 - IPS (Intrusion Protection System)
 - HIDS (Host Intrusion Detection System)
 - Antivirus

The user departments can avail this service. The scheme also has the provision to provide required licenses for HIDS and Anti-Virus. But for that, the User Department has to get in touch with the SIA to get the availability of the same. However in case the user department needs any specific security component to further fortify the security they shall be allowed to do so, at their own behest.

- ii. **Backup Services:** The SDC is equipped with shared storage and associated backup infrastructure which shall be backed up as per the backup policy of the State Data Centre. The department may leverage the backup server infrastructure for backup related tasks.
- iii. **Vendor Management:** The DCO may be required to provide vendor management support to the departments who seek this service. It must be noted that the user departments would not like to avail any services which overlaps with their existing service contract and lead

to multiple ownerships. However, in case the departments require this service then as per the severity level / escalation mechanism agreed with the user department the DCO shall provide vendor management services.

- iv. **Basic Hardware and OS level support:** Limited support from the Data Centre Operator shall be available for basic hardware related issues/vendor coordination and operating system level support if needed by the department.
- v. **Storage configuration and management:** The services to the department related to storage space management, configuration, and enhancement shall be available.
- vi. **Helpdesk Services:** The help desk service will serve as a single point of contact for all ICT related incidents and service requests. The service will provide a Single Point of Contact (SPOC) and also resolution of incidents. This can be leveraged by the departments IT team/vendors/Sis for any remote support, assistance in associated hosted infrastructure.
- vii. **Common IT Support Services:** This would include the common support services including patch management, antivirus management, updates etc.
- viii. **Monitoring:** An Enterprise Management System (EMS) has been procured for performance and health monitoring of the systems. Therefore, depending upon the mutual agreement with the user department, the DCO can offer end to end monitoring of the infrastructure and provide alerts / information as per the escalation mechanism mutually agreed. At present, EMS licenses for the IT Infrastructure provisioned for the SDC scheme have been considered. Further, in case the User Department needs to get the services of EMS monitoring the SIA can provision the same based on its requirements, under intimation to the Composite Team for support.
- ix. **Disaster Recovery:** It has been identified that NIC shall facilitate the DR Site for data replication and recovery for the SDC. 4 National Data Centres (NDC) shall cater to the DR requirements of 8 SDCs. Initial storage and server requirements expected by the SDCs for the same have been provisioned as part of an SDC Enhancement initiative of DIT, GoI.
- x. **Directory Services:** Directory servers available in SDC can be available on shared basis for departmental needs. It shall include Domain management, Group management, User management, Implementation of policies and standards etc.

Application Hosting Models

The services as mentioned in the section above can be leveraged in different application hosting models. These models give an initial indication of services covered in each and the manner in which these need to be deployed. However, depending upon the need, the SIA/ CT, DCO and the line departments may arrive at mutually agreed models and services in the portfolio. Three

hosting scenarios may exist that may impact the decision of the line departments while hosting their applications in SDC. These three scenarios have been evolved keeping in view the different implementation models for application deployment. These three models would include:

Co – location

- The user departments shall only require the physical and external connectivity infrastructure of the data centre to host their applications
- The Data Centre operator (DCO) shall ensure availability of entire core infrastructure and assist in Co – location of the application of the application. Respective application infrastructure shall be brought by the user Departments

Shared

- Some of the shared infrastructure (SAN & Compute) shall be used by the User Departments
- Application development & maintenance shall be taken care by the User Departments
- The DCO with support from CT shall agree upon the operations and management services required by the User Departments

Cloud Enabled Services

- Private Clouds shall be created for each State and State shall act as a Cloud service provider for User Departments, providing Infrastructure, Platform, and Software as a Service
- Self – service provisioning portal shall be extended to User Departments using Cloud services

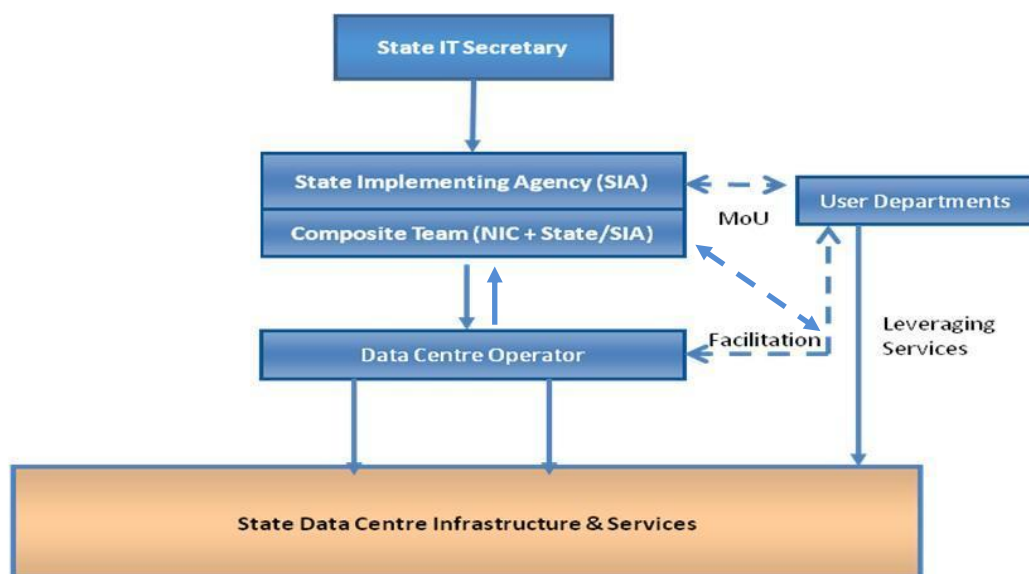
Depending upon the above scenarios/models, the specific services and the scope of agencies involved would need to be detailed and worked out at the State level. ***For all the above mentioned hosting models, The SIA / CT is required to finalize the Service Level Agreements (SLAs) with the line departments for hosting their applications.***

DIT is in the process of extending the Private Cloud in SDCs in a limited way. This will help the States to adopt innovative ways of utilizing this initial compute provided to them for enabling “Shared Services” to accommodate peak loads of departmental applications. This model allows the departments to configure the application infrastructure for normal load and not on peak load thereby enabling optimal usage of the infrastructure. This should rather be encouraged and adopted by the States to reduce power requirements, cost reductions and effective/optimal utilization.

It is therefore prudent to realize that the States/ UTs depending upon their maturity and need will evolve models for utilization of the compute equipment that has been provisioned as part of this scheme. For certain States /UTs it may be worthwhile to consider using some of this compute for other NeGP MMPs. For this the user departments, SeMTs and Composite Team can render expert advice and support to the States.

Stakeholders and their responsibilities

The key stakeholders which would get involved for application hosting purposes, their key relationships are shown below:



State Implementing Agency: The SIA as designated by the State Government shall be the implementing agency for SDC in the State. The SIA is responsible for the project implementation and functioning of the SDC. Depending upon the hosting requirements, the specific services and the scope of agencies involved would need to be detailed and worked out at the State level. For all the above mentioned hosting models, The SIA / CT would facilitate finalizing the Service Level Agreements (SLAs) with the line departments for hosting their applications.

Data Centre Operator: The DCO at the State is responsible for implementation and overall operations and management support for the State Data Centre. The DCO shall provide various services based on the agreed SLA with the SIA. Also, the DCO shall facilitate various common shared services, disaster recovery requirements and shall enable hosting of the application through agreed models and associated service levels.

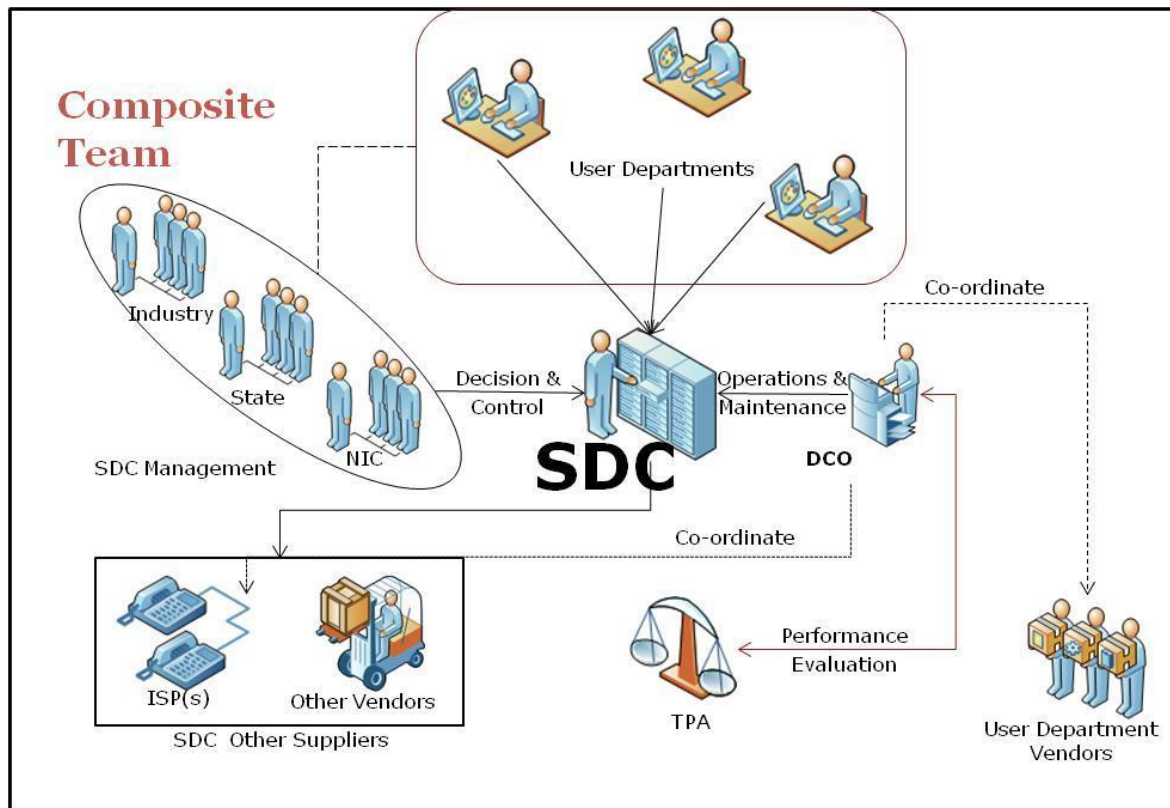
Composite Team : This team shall have members from NIC, SIA and may have professionals hired from market. This shall play a strategic role for management of critical infrastructure and also during the overall operations and management phase of the State Data Centre.

User Departments: User departments play a critical role in service delivery through SDC, as their application would be hosted at the Data Center under different hosting models described earlier in this document. The user departments shall arrive at their requirements for application infrastructure and accordingly would be agreed with SIA for hosting purposes.

The DCO, SIA and Composite team together would define the basic checklist which would be required to be met by the user department for application hosting in the SDC. This may include some essential areas including data security and privacy, access authorization, strategic control etc. DIT is in the process of preparation of a Service catalogue document which will simplify the

task by the State in making a provision for the Resources to the User Departments from the Available Resources

A draft Responsibility Matrix for all relevant Stakeholders is available at Annexure I.



Conclusion

The server and storage space being provided under the scheme can be utilized for hosting the State level applications either available with department or outsourced to vendors and this decision can be taken as per the mutual agreement between the departments and SIA/CT. It may be seen that the existing compute infrastructure provided to the States shall enable them to host their identified application for FAT and any other applications which are ready to be hosted at the Data Centre.

Further, the existing physical infrastructure being procured for the Data Centre shall give the Rack space and the basic Data Center Infrastructure services (storage, power, cooling, physical security, etc) to the line departments hosting their applications at the Data Centre. The physical space in the server farm area shall be fully equipped with power, cooling, fire prevention, CCTV coverage, access control etc to cater the requirement of the various departments.

Therefore there is ample rack space and infrastructure available with the States to host most of the existing / planned eGovernance application in the State Data centre. However the States would need to do the capacity assessment and utilize the existing racks for hosting the server and storage infrastructure procured under the scheme and the remaining may be utilized for collocation purpose as required. Some States may also decide to opt for virtualization wherein the departments can configure the application infrastructure for normal load and not on peak load thereby enabling optimal usage of

the infrastructure leading to a significant increase in the number of applications that may be hosted at the Data Centre within the existing compute infrastructure.

There is a need for the States to have a clear understanding of the potential of SDC and the available resources, so that there is no ambiguity for the same and optimum utilization of resources takes place. The State IT departments should also have clarity on how they will be extending the services of the Data Centre based on their application hosting plan. Further, it should also be understood that any incremental requirements in terms of servers, hardware, software etc would need to be provisioned by the State. However, the SDC scheme has provision for incremental requirements for software licenses and up gradations for the infrastructure bought under the SDC scheme at the State / UT.

Annexure I

Responsibility Matrix for Application Hosting at the SDC

Each activity shall have the involvement of multiple stakeholders. However, ownership of the same would differ and the roles of participating stakeholders shall be different, as defined below:

A – Advice (Advisory / Monitoring Role)

The Advisory role for any entity is such where the primary responsibility to execute the activity lies with someone else, and the advising entity is required to provide inputs and advice, whenever referred to by the primary stakeholder

E – Execute (Primary ownership)

Any entity responsible for executing any activity shall be the primary stakeholder for the same, and it is the said entity's responsibility to liaison with other stakeholders for coordination and inputs / advice for the execution & successful closure of the activity.

C – Coordinate (Performing activities as directed / discussed)

The coordinating entity shall assist the primary stakeholder(s) (i.e., the activity executing entity) in successful execution of the tagged activity including performing various tasks for the completion as deemed required for the activity.

S No.	Activity	Stakeholder			NIC
		User Department / Application Developer	DCO	State and Composite Team	
1	Application Design, Development, Testing and Release	E			
2	Infrastructure finalization for Application	E		A	
3	Finalization of Infrastructure requirements at SDC	E	C	E	
4	Application Hosting Testing in Staging Environment and Application Security Certification	E	C	C	
5	Application Migration to SDC Live Environment	E	C	C	
6	Application connectivity to SAN, and other common SDC Modules, and Web	C	E	C	

S No.	Activity	Stakeholder			NIC
		User Department / Application Developer	DCO	State and Composite Team	
	Connectivity (as applicable)				
7	Performance and Health Monitoring	C	E	A	
8	Error Reporting and Patch Management	E(Remote)	E (Helpdesk)	C	
9	Ensuring Power, cooling, available common SDC security, and Web & SWAN & SAN, connectivity, as applicable, to Application Servers		E		
10	Assessment of Application criticality for Disaster Recovery inclusion	E	C	E	
11	Application bringup at DR Site	E		C	C
12	Application resumption at SDC Site	E	C		

Annexure II

Infrastructure Availability at the SDC

S. No	Infrastructure at SDC	Description
1	Server Racks/ Rack Space	42U or 38 U racks will be available at SDC with 4.5 KVA at each Racks
2	SAN Storage	Sufficient scalability is provisioned under SAN for 5 years requirement
3	SAN Switches	Two redundant SAN switches are available. The ports for the same can be provisioned for connectivity can be extended based on the availability.
4	KVM Switch	IP/ Non-IP KVM Switches are available. The services from the same can be extended based on the availability.
5	Cables & Connectors	Structured cabling has been provisioned for the entire Server Farm Area as per the number of Racks than can be accommodated (24 port/ Rack)
6	Networks & Security	L3 Switch Perimeter Firewall IPS / IDS L2 Switches Antivirus HIPS
10	PDU (power strip)	10/15 socket per Rack of 16 Amp each are provisioned in each Rack in SDC
11	Backup Software	Backup software is already provisioned in SDC, only required licenses need to be provisioned. Limited Tape drives have been provisioned, more Tape drives have to be provisioned based on the requirement.
12	Monitoring Software (EMS)	Performance and health monitoring can be extended through the existing EMS in the SDC.

*Note: Limited Compute (5 App Servers, 5 DB Servers, 2 Web Servers) have been provisioned under the scheme, application that will used for Final Acceptance Test will be utilizing some of these servers. The MMPs can contact the SIA/ CT for checking the availability of the existing compute. Detail is enclosed in the Annexure III. The scalability of infrastructure that have been provisioned under the SDC scheme for the State, is prepared keeping in mind the requirement for User departments, State Government and MMPs applications that are expected to be hosted in SDC.

Each MMP and State Department is required to contact the State Composite Team with details of the required components at the SDC and check the availability of the same. Further is being motivated to the State User Departments to get in touch with the State Composite Team and start deploying the application and infrastructure which are ready to be migrated to State Data Centre.

Annexure III

Compute Provisioned in SDC as part of SDC Scheme

S. No	Components	Qty
<u>Server Details</u>		
1.	Application Servers	5
2.	Web Servers	2
3.	Database Server (Intel / AMD 64) and (RISC/ EPIC)	5
4.	Enterprise Access Server	2
5.	Management Server	1
6.	Directory Server	2
7.	Enterprise Backup server	1
8.	Antivirus Server	1
9.	Staging Server	1
10.	Integration Server	1
11.	IPS server	2

* The above content and number may change State to State (as per the approval in the DPR)