No. 10(6)/09-EG-II
Government of India
Ministry of Communications and Information Technology
Department of Information Technology
Electronics Niketan
6, CGO Complex
****

New Delhi-110003
November 16, 2010

Circular

Guidelines for Strategic Control in Outsourced Projects

The National e-Governance Plan of Indian Government seeks to lay the foundation and provide the impetus for long-term growth of e-Governance within the country. The plan seeks to create the right governance and institutional mechanisms, to set up the core infrastructure, to develop policies and to implement a number of Central, State and Integrated Mission Mode Projects with defined service levels in order to create a citizen-centric environment for governance. Implementation of e-Governance projects is a highly complex process requiring provisioning of hardware & software, networking, change management and capacity building.

To expedite the implementation e-Governance projects, participation of Industry both as partner and vendor has become essential. This has resulted into a significant increase in the role and responsibilities of the Industry and Private Sector in such projects. Although outsourcing to Industry has increased the capacity for implementation of the projects, it has also necessitated the need to focus on retaining Strategic Control within the Line Ministries/Departments of the Government.

Strategic Control enables Line Ministries/Departments to have control over the outcomes, make required changes and have the capability of exit management. Additionally it also ensures that the Government has complete control over the Strategic Assets like software application, databases and core infrastructure. It therefore becomes highly imperative for the government to ensure proper systems, processes and structures are put in place so the government can exercise Strategic Control over the entire lifecycle of the programs starting from conceptualization to operation and maintenance.

A need was therefore felt to lay down guidelines for Strategic Control in Outsourced Projects which will provide the necessary tools and techniques to the Line Ministries and Government Departments to ensure Strategic Control of the e-Government Projects and achieve the vision of the National e-Government Program in a sustainable and time bound manner. These guidelines have been developed after wide consultations and are being circulated as a guide for all e-Governance projects.

(Anurag Goyal)
Director

Encl: Guidelines for Strategic Control in Outsourced Projects

To:

All Ministries and Departments of the Government of India

IT Secretaries of all State Governments and UTs

Guidelines
For
Strategic Control
In
Outsourced Projects

Department of Information Technology,
Ministry of Communications and IT,
Government of India

Published: November-2010

Foreword

The National e-Governance Plan of Indian Government seeks to lay the foundation and provide the impetus for long-term growth of e-Governance within the country. The plan seeks to create the right governance and institutional mechanisms, to set up the core infrastructure and policies and to implement a number of Central, State and Integrated Mission Mode Projects, with well defined service levels, to create a citizen-centric and business-centric environment for governance. Implementation of e-Governance projects is a highly complex process requiring provisioning of hardware & software, networking, change management and capacity building.

To expedite the implementation e-Governance projects, participation of Industry both as partner and vendor has become essential. This has resulted into a significant increase in the role and responsibilities of the Industry and Private Sector in such projects. Although outsourcing to Industry has increased the bandwidth for implementation of the projects, it has also necessitated the need of retaining Strategic Control within the Line Ministries/Departments of the Government.

Strategic Control enables Line Ministries/Departments to have control over the outcomes, make required changes and have the capability of exit management. Additionally it also ensures that the Government has complete control over the Strategic Assets like software application, databases and core infrastructure.

While the government implements the e-governance projects through outsourced agencies, it becomes highly imperative for the government to ensure proper systems, processes and structures are put in place so the government can exercise Strategic Control over the entire lifecycle of the programs starting from conceptualization to operation and maintenance.

This document will provide the necessary tool and techniques to the Line Ministries and Government Departments to ensure that they retain the Strategic Control of the e-Government Projects and achieve the vision of the National e-Government Program in a sustainable and fast manner.

Table of Contents

1. Introduction

1.1 Information Technology (IT) has emerged as a key driver in improving the efficiency in the Government Processes thereby facilitating higher levels of service delivery to the citizens and other stakeholders. Additionally, it is also improving the effectiveness, accountability and transparency of the Government processes. To expedite the implementation of IT projects especially in the area of e-Governance, participation of Industry both as partner and vendor has become essential. This has resulted into a significant increase in the role and responsibilities of the Industry and Private Sector in such projects. Although outsourcing to Industry has increased the bandwidth for implementation of the projects, it has also necessitated the need of retaining Strategic Control within the Line Ministries/Departments over the project life cycle, its deliverables and outcome.

1.2 This document details out necessary guidelines enabling Line Ministries/Departments to retain Strategic Control within the Government framework.

1.3 Although Strategic Control has not been formally defined anywhere, however, it is about Line Ministry/Department having control over the **outcomes** and ability to make required **changes**, **enhancements**, and having capability of **exit management**. Additionally, it could be interpreted as the authority of the Government to have complete control over the **Strategic Assets**, i.e., software application, databases and core infrastructure. This also means that:

i. The system performs functions and acts in conformance with the requirements and provides desired outcomes (deliverables/Service Levels).

ii. The application system and the databases are designed, developed, installed and managed exactly in conformance with the procedures laid down for delivery of services.

iii. The security of the overall system is of the appropriate order following international standards.

iv. Any change required to the solution is with specific approval of competent authority in the Government.

v. The outsourced vendor does not have access to the system beyond prescribed authority as defined by Line Ministry/Department.

vi. The processes, including legal enablement and capacity within the government are in place to take-over the entire system in case of an exit of the vendor (premature or planned).

vii. There is an ability to make necessary mid-course changes to the system

1.4 To address the requirement and for day-to-day monitoring to check the efficacy of Strategic Control of the assets, the Government would need to:

i. have complete understanding and knowledge of the system

ii. possess necessary documentation of the architecture, design and functioning of the system

iii. have right kind of tools to monitor the system, specifically related to Strategic Assets.

iv. have complete ownership over the data

v. possess optimum manpower and required capability to monitor and scale up for taking over the system, whenever required. The manpower required would be in the area of:

- Application Related expertise
- Data and Database related expertise

- System related expertise
- Data centre related expertise
- Networking related expertise
- Security related expertise

1.5 The following are the measures needed to ensure the required Strategic Control in outsourced project:

i. The need and contours of Strategic Control should be defined at the conceptualisation stage itself.

ii. Design of the project is such as to ensure vendor independence.

iii. Ensure security and privacy of the Government data by retaining complete control on data/information

iv. minimize vendor lock-in and provide viable exit management process through knowledge of tools, technologies and architecture for necessary control on applications software to

v. The Qualification Criteria for prospective outsourced vendors are set based on the nature of the project.

vi. Necessary arrangements for monitoring of adherence to SLA are made for the operations and maintenance of projects.

2. What are Strategic Assets?

Following may be classified as Strategic Assets which require necessary control of the Government:

i. Software application, Data, Databases and Core Infrastructure.

ii. The knowledge and processes applied during design and implementation.

iii. Resources and tools that help in managing the application.

iv. Intellectual Property created during the lifecycle of the project.

3. Objectives of Strategic Control in projects managed in Outsourced Mode

Strategic Control in projects managed in outsourced mode should ensure the following for the Government:

i. Control over Governance Process, Information and Outcomes.

ii. Control over all intellectual property, source code and associated documents.

iii. Non leakage of Revenue and Information.

iv. Control over security processes for data, application and infrastructure security and integrity.

v. Control of Service Levels and their monitoring.

vi. Making necessary changes and enhancements as and when required as per business needs.

vii. Complete control over audit trails.

viii. Taking over the system with ease whenever required due to exit of private partner.

4. Governance Structure

Governance Structure depicted in Figure **1** is suggested in the Operational Guidelines[1] issued by Dept. of IT, GoI. This section describes various elements of Governance Structure which have to be leveraged for retaining the Strategic Control within the Line Ministry/Department. Further details on Governance Structure including Roles and Responsibilities are provided in Operational Guidelines. The suggested Governance Structure is mentioned below.

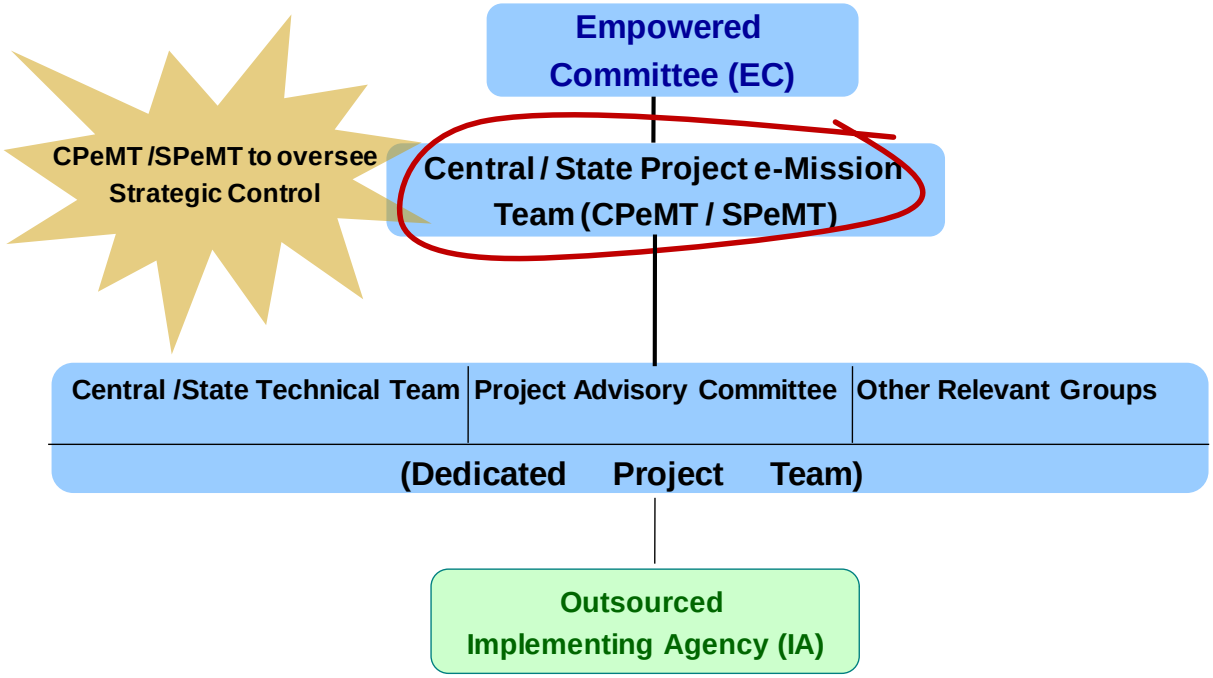


Figure 1 - Governance Structure (Based on Operational Guidelines)

Empowered Committee (EC), with Secretary of the Line Ministry as its Chairman, shall be responsible for overall guidance, for deciding policy level matters and to act as final body for approving all deliverables relating to the Programme.

Central Project e-Mission Team (CPeMT) is headed by a senior domain representative from the Line Ministry as the Project Mission Leader. The Central Project e-Mission Team (CPeMT) has the overall responsibility of project design, development, supervision, guidance, evaluation and monitoring of the implementation, business process re-engineering implementation of an e-Governance project and shall be responsible for exercising Strategic Control. To effectively manage various activities of the project development and implementation, various subgroups could be formed under CPeMT to support its activities. The two key subgroups are Central Technical Team (CTT) and Process Advisory Committee (PAC).

- **Central Technical Team (CTT)**: The responsibility of CTT inter alia includes providing technical leadership and **ensuring** Strategic Control over the project and Strategic Assets.

[1] The Guidelines are available at the URL http://mit.gov.in/download/GuideforOperationalModel4.0.pdf

- **Process Advisory Committee (PAC):** PAC is responsible for providing process level inputs and functional requirements.

Implementation Agency (IA): IA, which can be an outsourced agency, is entrusted with the responsibility to undertake implementation of the project as per predetermined deliverables. IA is accountable to CPeMT through CTT and PAC. Detailed process and responsibilities of IA, CTT and PAC are mentioned in Operational Guidelines.

Programme Management Unit (PMU) or a **Special Purpose Vehicle (SPV)** could be created in order to provide operational flexibility and financial autonomy in monitoring and implementation of the project. PMU or SPV also facilitates engagement of skilled resources from the market to strengthen CPeMT/CTT on need basis.

Dedicated Project Team: In order to have a unified and integrated support to all e-Governance/ICT related initiatives within the Line Ministry/Department, there is a need to create the above mentioned sustainable institutional framework. Towards this objective, the CTT, PAC and other groups will be dedicated to the project on a full time basis working as a 'Dedicated Project Team'. Based on the complexity of the project, a member of the Dedicated Project Team may be dedicated for documentation of the project. The dedicated project team could be a part of the CPeMT for smaller project or could be constituted in the form of a SPV for a very large projects based on the requirements of the respective Department. This team shall have following key responsibilities at the program level -

- Provide a unified & integrated approach to all ICT related initiatives
- Support in ensuring Strategic Control
- Address cyber security
- Ensure Standards and interoperability
- Administer best practices
- Administer policies and procedures across projects
- Ensure use of common infrastructure

The detailed roles of the CPeMT and CTT for the purpose of retaining Strategic Control are further elaborated in para 4.1 and 4.2 respectively.

The teams corresponding to CPeMT and CTT at the State level are State Project e-Mission Team (State PeMT) and State Technical Team (STT).

4.1. Central Project e-Mission Team (CPeMT) / State Project e-Mission Team (State PeMT)

a) Formation of CPeMT – The CPeMT is normally headed by a senior domain representative from the Line Ministry (not below the level of Joint Secretary) as the Project Mission Leader. It is expected to have senior representatives from the Line Department, State Government, NIC, DIT, NISG and others. For more details, refer to Operational Guidelines issued by Department of IT[2].

b) The continuity of the key members of CPeMT is critical for the success of the project and therefore it should be maintained all through the complete life-cycle of the project. Depending upon the type of project, senior members from Industry bodies such as NASSCOM, MAIT may be included as special invitees in CPeMT. However, the Line Ministry/Department should ensure that no conflict of interest arises out of such inclusions.

[2] The Guidelines are available at the URL http://mit.gov.in/download/GuideforOperationalModel4.0.pdf.

c) The Central Project e-Mission Team (CPeMT), established at the Central Line Ministry to manage and monitor all activities with respect to design, development, implementation and roll-out of the Project Scheme, shall be made responsible for clearly defining the level and extent of Strategic Control. CPeMT shall ensure Strategic Control of the project with support of CTT.

d) For the purpose of **ensuring Strategic Control** over the project CPeMT shall:
   i. Decide on the **contours of Strategic Control**. CPeMT in the very beginning itself should assess and approve the criticality of the project with respect to Strategic Control as worked out by CTT.
   ii. Define the **extent of IPR** of application software based on the criticality and commercial aspects of the system.
   iii. Be responsible for entire project design and development, including key deliverables, SLAs and outcomes.
   iv. Develop the business structure for industry participation (private enterprises including participation of foreign organization) in projects to be outsourced.

e) The CPeMT should ensure regular review meetings at scheduled frequency. All meetings shall be duly minuted, which shall be submitted and presented to the EC in a time bound manner.

4.2. Central Technical Team (CTT) / State Technical Team (STT)

a) Formation of the CTT - The CTT is primarily a technical body that may be headed by a senior technical member, nominated by Mission Leader/Line Ministry as Chairman. CTT shall also have requisite number of internal/hired IT experts. The composition of CTT is described in detail in Operational Guidelines. CTT is expected to critically review and supervise the basic design of the system and, while doing so, has to ensure effective Strategic Control as defined by the CPeMT.

b) From the perspective of maintaining Strategic Control, the CTT's role is as follows,
   (i) Ensure standards for S/W development
   (ii) Ensure Strategic control as per the contours decided by CPeMT
   (iii) Ensure taking over of IPR (extent as decided by the CPeMT), and necessary knowledge of COTS packages if used.
   (iv) Interface with third party certifying agency
   (v) Manage knowledge transfer from consulting and implementing agencies.
   (vi) Detail the criticality of various project components/modules within the framework and contours of Strategic Control as decided by CPeMT.

c) The control over Strategic Assets would be achieved by ensuring:
   (i) Core application and databases are owned by the Government and changes to the application system/databases are made only under due authority of the Government.
   (ii) Control over network as well as security system (by way of assigning roles and privileges, configuration management in relation to all the security assets like firewalls, routers, switches, IPS and IDS).
   (iii) Planning for Exit Management, wherein the Government has thorough understanding of the System and is in a position to scale up and take over the system, whenever required.

(iv) Auditing and testing by STQC/3rd party Independent Auditors with the help of internal or external resources.

(v) Detailed documentation created for the project by the outsourced implementing agency, in consultation with CTT/PAC for the entire lifecycle of the project shall remain under the ownership of the CTT.

5. Levels of Strategic Control

A project is usually broken down into several logical components (modules or services) that interface with each other to give the overall functionality. From the Strategic Control and security perspective, it becomes essential to categorize each of these project components. Government of India has formulated standards and guidelines to ensure information security in e-Governance projects. This includes e-Security Assurance Framework for Security Categorisation of Information System, which provides a generalized format for expressing the security category (SC) of software application.[3] It could be used to categorise an e-Governance project based on potential impacts to the organization in case of security needs.

On the similar lines, a project may be categorised for defining the contours of Strategic Control. The Strategic Control category could be defined by considering the attributes such as –

- Exposure to National Security (External)
- Exposure to National Security (Internal)
- Sensitivity of Governance Workflow
- Criticality of Data and Information
- Extent of Financial Exposure

Other attributes could also be considered based on the needs and requirements of specific Line Ministry/Department. Each of these attributes should be categorised as Very High, High, Moderate or Low to arrive at overall categorisation of Strategic Control requirements for the project. This activity shall be performed by CPeMT during conceptualisation stage of the project. For illustrative examples to be used as a guide refer to Annexure D.

i) Category 1 – Low Level

A low-impact project is defined as one for which all of the criteria are low. All components of the project are low impact. At least CTT shall have necessary knowledge and overall understanding of the architecture and the design.

ii) Category 2 – Moderate Level

A moderate-impact project is defined as one for which at least one of the criterion is moderate and no criterion is more than moderate. None of the components has very high or high impact. At least CTT shall have understanding of architecture and the design with knowledge of tools and methodologies used. The project could be outsourced to a lead vendor with one or more sub-

[3] Guidelines for Security Categorization of eGovernance Information Systems, eSAFE-GD100, Ver 1.0, January 2010, DIT, GOI, available at http://egovstandards.gov.in/approved-standards/egscontent.2010-02-25.2041424279/base_view (URL Accessed 01 June 2010)

vendors to enable backup(s). Data accessibility should be allowed to limited and vetted personnel from the vendors.

iii) Category 3 – High Level

A high-impact project is defined as one with at least one of the criterion as high or any one of the component has high impact. In addition to the understanding of architecture, high level and detailed design with knowledge of tools and methodologies used, CTT should participate with outsourced vendor in design and development of the system. Implementation and rollout of the system could be outsourced to multiple vendors. Data should be supervised/managed by CTT/supported by Government body.

iv) Category 4 – Very High Level

A very high-impact project is defined as one with at least one of the criterion as very high or any one of the component has very high impact. CTT along with Government body supervise the vendor(s) or a Government body, like NIC, could be chosen for solution development. The critical data should be managed internally by the Government Department.

For further details about Level of Strategic Control please refer Annexure E.

6. Phase-wise actions for Strategic Control

6.1. Project Lifecycle

A typical project lifecycle has following phases:

i. Project Conceptualisation
ii. Detailed Project Report
iii. RFP and Scope Development
iv. Bid Evaluation and Selection
v. SRS Development
vi. Design and Coding
vii. Testing
viii. Operations and Maintenance
ix. Exit Management

Strategic Control has to be managed over the entire life cycle of the project beginning from conceptualisation stage, definition of functional requirements, architecture, application development and right up to operations and maintenance phase. Foundation of Strategic Control for any outsourced project is laid down by Line Ministry/Department at the time of Project Conceptualisation.

6.2. Processes common to all phases

This section indicates the steps that need to be taken by States / Government Departments to ensure Strategic Control over technology assets during a project that is managed in a Public-Private Partnership mode.

The Strategic Control will have to be retained on a continuous basis within the Line Ministries/Departments. Usually, as applications evolve due to continuous re-engineering of the processes, the application software also will keep evolving over time. Such changes in processes and consequent changes in application also have to be retained within the Line Ministry/Department as part of the Strategic Control.

For all phases, following common principles should be used to retain Strategic Control,

i. **Project tracking** - For this, project planning tools can be used. The IT software vendor should share the tool and status dashboard with the CTT to ensure transparency.

ii. **Review Process** – All phases should have peer and management reviews. All documents, design and code should be allowed after critical review of the same.

iii. **Phase-End Approval –** Each Phase should be formally approved as completed by the CTT/STT. The CPeMT / State PeMT should monitor these approvals.

iv. **Configuration Management** process to ensure that all changes (in code and in documents) are version controlled. All version increments should be marked with name of person making change, reason for change along with date and timestamp.

v. **Release Management process** should be adopted at all suitable phases.

vi. **Use of Standards** – Project processes and controls should be based on standards. For more details on e-Governance Standards, please refer to the following link: http://egovstandards.gov.in/. For software asset management, standards like ISO/IEC 19770 may be followed.

vii. **Security Provisions** – The vendor should abide by well defined security processes. Standards like BS7799 / ISO27001 may be used as benchmarks. Please see Annexure A for details.

viii. **Documentation** – Rigorous documentation should be followed. Please check Annexure B for an indicative list of documents that the CTT should ask the vendor to provide.

ix. **Project repository** to store all related documents/artifacts/version control.

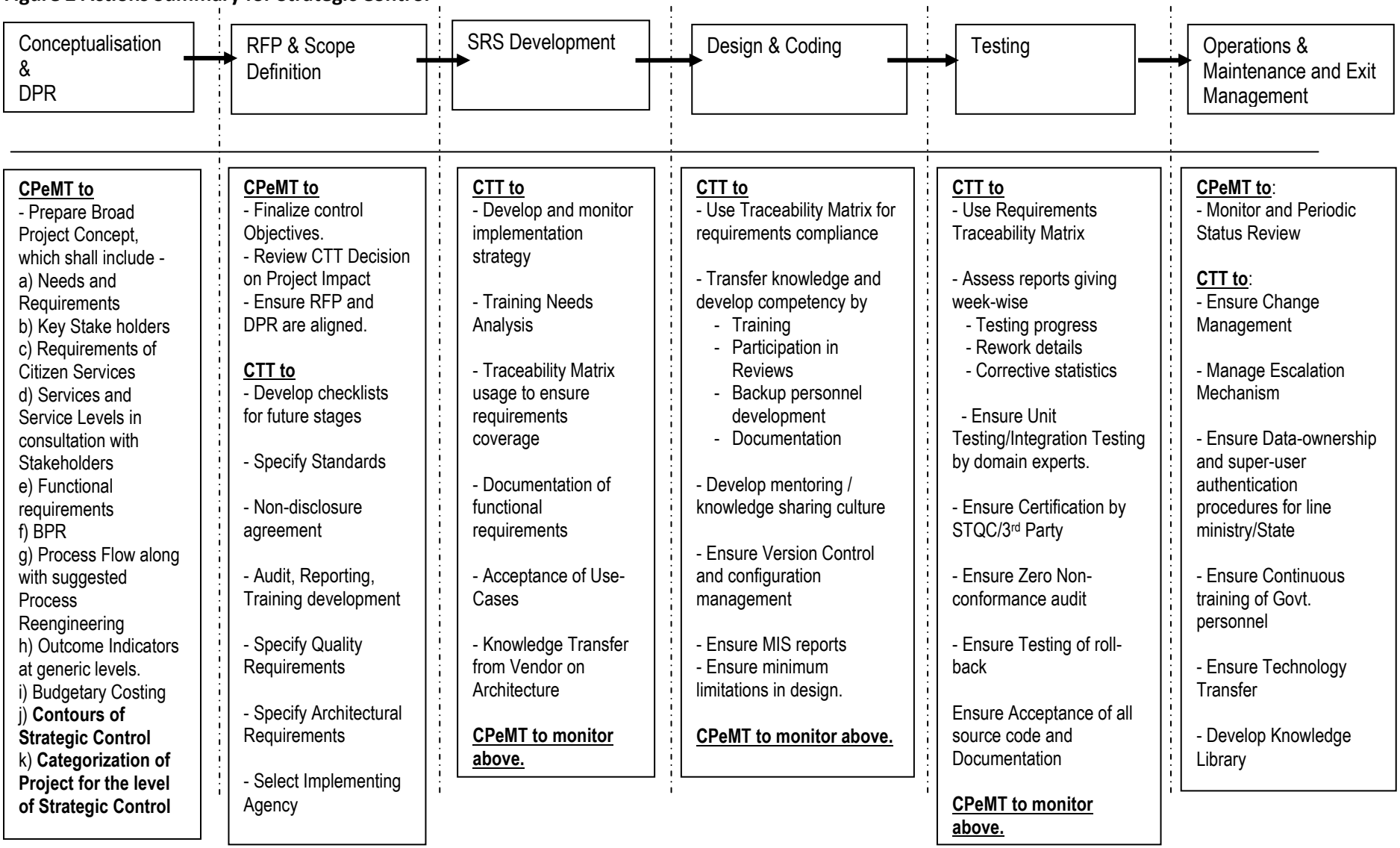
x. During the Bid Evaluation, CPeMT should be involved in order to ensure that Strategic Control objectives are met.

xi. **Disaster Recovery and Business Continuity Planning** – This should be tracked as a part of development of Strategic Control. Appropriate geographical distribution, backup planning and regular risk assessment should be carried out under this.

6.3. Steps detailed out in phased-wise actions for Strategic Control requires following mechanism:

- Strategic Control is to be managed by the Line Ministries/Departments over the entire life cycle of the project beginning from conceptualisation stage to technology selection to actual development and maintenance, not just in application development.
- In-house capability in terms of requisite number of technical resources within the Government for managing Strategic Control of an outsourced activity.
- The team managing the Strategic Control would be under the supervision and control of head of the dedicated team executing the project who is required to have adequate techno-managerial knowledge and experience.

Figure 2 Actions Summary for Strategic Control



6.4. Processes specific to phases during project life-cycle

The following tables enlist the needs in each phase of a project and suggest ways to accomplish them. The table is indicative and may be modified as needed.

Table 1 - RFP and Scope Definition Stage Guidelines

What needs to be accomplished in this stage?	**How? - Steps/Suggestions to ensure the needs are accomplished**
- CPeMT to finalize the objectives on the degree of Strategic Control - CPeMT to ensure that DPR requirements are covered here. - CPeMT to ensure that capacity for Strategic Control is built during project timeline - CTT to develop documentation list - CTT to specify usage of standards and security systems	- Identification and categorization of project modules and decision on their control. - Assignment of qualified personnel from CPeMT - Usage of checklists for important documents - Use of standards as communicated by DIT Provision for Knowledge transfer to client at every stage of project - Deliverable acceptance mechanism may be defined or for a defined acceptance process, the same should be used for each deliverable identified at the beginning of the project.
Non Functional Requirements - Security and Access Control - Business Domain Requirements - Quality Requirements - Technical Requirements	- Non-disclosure agreement between Govt. and vendor (Please checkAnnexure A for more details) - Reporting, Audit, Search, Training, Payment, Content Management, etc. - Quality should cover usability requirements, standards, performance and scalability parameters etc. - Technical requirements will include Enterprise Architecture, Service Oriented Architecture, Interoperability Requirements, Metadata, etc.

Table 2 - SRS Stage Guidelines[4]

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
CTT should ensure that, - The SRS correctly translates business requirements into functionalities and capabilities that the proposed software system must provide. - SRS is a combination of, - Functional Requirements - Planned Architecture including application architecture, database architecture, database control, network architecture etc. - User Access rights - Functional Modules - Use Cases - Scenarios - Data Requirements - Others	The CTT should use traceability matrix to ensure completeness and consistency of the SRS. Please check the sample matrix in Annexure C. The CTT should ensure acceptance and sign-off of following, - Documentation of the functional requirements - Acceptance of the use-cases - Knowledge transfer and awareness on architecture (database, network, applications etc.) - SRS approval. CPeMT should monitor and guide CTT as necessary.

It is imperative to note here that the Traceability Matrix evolves as the project progresses. Therefore, the CTT should ensure versioning of Traceability Matrix to track changes at each stage. CPeMT should monitor these changes to ensure that they do not deviate from the Scope of the project.

[4] This section derives heavily from SRS Template developed by NISG in NISG 1001:2008 document. Readers are encouraged to use the same during SRS development phase.

Table 3 – High Level Design Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
Following are described and used generally in the HLD, - User Interface - Dataflow Diagrams - Other system components - Integrate with COTS (if used as building blocks).	CTT needs to ensure, - Prior Knowledge - Training - Involvement with the vendor during HLD development
- Software development methodology and tools	- Competency development in CTT and Departments using training / mentoring to ensure full understanding of the development methodologies. - In addition to the above, training to develop competency in tools used for software design may also be needed.
- Create Knowledge Banks to "Preserve" domain knowledge	- CTT Personnel should - participate in review - ensure continuity - nominate more than 1 person - ensure proper documentation - Culture of sharing / mentoring to be fostered

Table 4 - Detailed Design Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
- Understanding of the detailed design The detailed design consists of description of - Data Structures - Database Design - Components and Entities - Interactions between components - Pseudo Code or Code Prototype - Design Limitations	CTT should ensure, - Awareness of system architecture and detailed design documentation. - Technical training if needed - Continue usage of the traceability matrix to map components with requirements CPeMT to monitor above.
- Map the detailed design to the business imperatives of the project - Ensure inclusion of - Workflow - Reports - Outputs - MIS requirements	CTT to ensure, - Use of traceability matrix developed during the SRS phase should be continued to ensure completeness. - Use Checklist to ensure that design limitations do not ***imply*** non-fulfillment of business requirements. CPeMT to monitor above.

Table 5 – Coding Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
Source Code will consist of, - Modules, - Libraries, - Packages as per the design	The CTT needs to, Understand - Standards and basic coding rules - Documentation, - Version control and - Configuration management. - Ensure appropriate security measures to avoid "leak" of important code parts. - Ensure compliance to detailed design and requirements (Traceability Matrix) Standards to be followed by the SI for coding and documentation and regular IT audits on the same. CPeMT to monitor above.

Table 6 – Unit Testing Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
- The CTT may seek assistance from STQC/3rd Party during UT. The responsibility of testing rests with user (represented, here, by the CTT) - All code units should exceed the minimum set conditions - All Boundary conditions, interactions, process flows, error conditions should be tested in addition to the basic functionality.	CPeMT and CTT should monitor, - Defect related statistical reports from all components/packages - Clear documentation of week-wise testing progress along with impact of failed testcases. - Test result summary to indicate the initial success, rework and corrective statistics. - Domain experts from the Line Ministry should also test the components for functional requirements

Table 7 – Integration Testing Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
Design and Code acceptance include transfer of, - Entire source code. - description of code architecture in documents and within code comments - Information about known pitfalls *Special attention to ensure,* - Security/authentication procedures are developed - All interfaces with legacy data are developed and transferred.	CTT should ensure following: - The domain experts test proper functionality - Required documentation is supplied (indicating the transferred code, authentication procedures and legacy data interfaces) CPeMT to monitor above.

Table 8 – UAT Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
UAT carried out by the vendor needs to be validated. - UAT Environment for Govt. to test on. - Rollback to legacy system should be tested to ensure that the overall service does not stop. Provision of rollback ensures the same. - Audit to check against security loopholes in system. - 100% Validation of requirements	CTT with help of STQC / 3rd Party shall, - Get system certification - Obtain audit Reports with Zero non-conformances. - Test failure of rollout and rollback should be explicitly documented **- "End User-centric" testing should be carried out to ensure that core objectives are met.** CPeMT to monitor above.

Table 9 – Operations & Maintenance Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
Supervisory Control on - System Administration - Network Administration - Database Administration - Changes and enhancements to system	CPeMT and CTT should monitor all O&M activity. - A weekly/periodic status review.
- Data Ownership by Line Ministry	- Authentication and super-user mechanism to prevent unauthorized viewing. Change management process should be defined and adhered to.
- Audit with logs preserved post event. A dashboard view of problems and complaints. - Auto escalation mechanisms to address above.	- Monitoring and analysis of Performance Reports.
Tools used for O&M, - Develop(or purchase COTS) tools to simplify management and maintenance of the new system	- Training of tools - Detailed user manual of tools
- This should include tools to - control change management - identity management - data integrity - audit processing	- Competency and training of tools and their deployment.

Table 10 – Exit Management Stage Guidelines

What needs to be accomplished in this stage?	**How?** **Steps/Suggestions to ensure the needs are accomplished**
CTT to - Ensure that capacity has been built with Government	- Transfer of Technology
- All assets have been taken over from vendor	- Knowledge transfer and management as per plan
- Non-disclosure agreement(s) signed by vendor CPeMT to monitor above.	

Annexure A - Strategic and Security Control in Outsourced Operations

This annexure provides a detailed analysis of security and access related issues in outsourced projects.

The 4 key factors which are essential in maintaining proper controls in an outsourced operation are – **People, Policies, Processes and Infrastructure**

1. **People**
    a. Organization structure
    b. Employee Contracts and non-disclosure agreements with vendor(s)
    c. Background check and screening of employees (presently being done in case of Defence contracts)
    d. Induction and regular training programmes to orient staff regarding Security measures.
    e. Supervisory control by Departmental/ Government staff.
    f. Attracting and retention of the right skills - To effectively manage the outsourced activities it is important to maintain the core skills internally.
        i. One way of retaining / building skills internally, retaining interest of staff and helping to build a common culture is through rotation of staff.
        ii. Strong motivators to attract talent:
            1. Challenging work in public sector
            2. Ability to develop new skills both on the job and through trainings.
        iii. Reward and recognition programs are important.
        iv. Two different pay scales for internal and external staff are considered to be a problem. The salary differential should not be more than 30%.

2. **Policies**
    a. Documented organization policies
    b. Role based authorities and access
    c. Data classification (critical, manageable & commodity)
    d. Role classification
    e. Decision making controls in line with the governance model.
    f. Design for proper security and controls
    g. Integration of security with delivery life cycle. Security policy should be comprehensive and should cover access privileges, encryption policies, vetting procedures (as indicated earlier), audit trails, network security etc.
    h. Emphasis on approved security frameworks and policies
    i. Strict penalties for non-compliance.
    j. If possible divide the job region wise to multiple vendors. This will maintain competitive environment and also back-up in case of any failure.

3. **Processes**
    a. Application specific access and security controls.
    b. Define core/non-core processes for management controls.
    c. Comprehensive logs of all operations / transactions and regular review
    d. Controls on database, network, OS etc
    e. Intellectual property protection
    f. Business continuity planning
    g. Regulatory compliance

h. Periodic Audits

4. Infrastructure

a. Define enterprise security standards.
b. Physical security and access controls
c. Network security, firewalls, perimeter and endpoint defenses.
d. Monitoring and compliance of security standards.
e. Detailed risk assessment.
f. Regular security audits.

One of the ways to reduce the risks is to break- up the outsourcing into in three steps:

a) Consulting and design
b) Implementation
c) Validation and verification

It is strongly recommended to have internal very strong experienced procurement and contract management skills. Domain knowledge of the business and governance comes internally from the implementing department.

Annexure B – Ownership of Documents

(Page 10/Sub-point viii)

The documentation is vital to any successful e-Governance project. Following is an indicative list of documents that the vendor should develop and share with CPeMT/CTT

- Detailed Project Report
- Detailed Project Management Plan
- Work Breakdown Structure
- Critical path Document
- Functional Requirements specifications
- Software Requirements specifications
- Software Configuration Management Plan
- Risk Management Plan
- Architectural Design Document
- Software Detailed Design Descriptions
- Infrastructure Requirements and Deployment Architecture specifications
- ISMS document
- Business Continuity Plan
- DR Plan
- ITIL/ITSM Plan
- Source Code/Documentation
- Unit Test Plan with Test Cases
- Integration Test Plan with Test Cases
- System Test Plan with Test Cases
- ITIL / ITSM based Operations & Maintenance manuals
- Policy documents
- User Manuals
- Exit Plan including the interim take over strategy and plan

Annexure C – Sample Requirements Traceability Matrix

(Page 13/Table 2)

The following template is adapted from the template available at the URL http://www.uservices.umn.edu/pmo/docs/Analyze/TEMPLATE_Requirements_Traceability_Matrix.xls (URL accessed on May 29, 2009)

An example traceability matrix for the phases described earlier is presented below:

< Name of the Project/MMP>			**<Name & Designation of Project Manager>**			
Phase ⟶ **Requirements**	**RFP**	**SRS**	**Design**	**Coding**	**Testing**	**Knowledge transfer at Exit**
Mandatory Requirements						
R1						
R2						
…						
Rn						
Optional Requirements						
O1						
O2						
…						
On						

The original traceability matrix available at above URL is given below.

UNIVERSITY OF MINNESOTA *University Services* program.management.office						
Requirements Traceability Matrix						

Project Name		Business Area	
Project Manager		Business Analyst Lead	
QA Lead		Target Implementation Date	

No.	Category / Functional Activity	Requirement Description	Use Case Reference	Design Document Reference	Code Module / Reference	Test Case Reference	User Acceptance Validation	Comments

Annexure D – Example of Levels of Strategic Control Definition

(Page 8/Para 2)

Example Categorization of Project/Components

Project / Project Attribute	**Project 1**	**Project 2**	**Project 3**	**Project 4**	**Project 5**	**Project 6**
Revenue Exposure	HIGH	LOW	LOW	LOW	LOW	LOW
Information & Data	MODERATE	HIGH	HIGH	LOW	MODERTATE	LOW
Governance Workflow	HIGH	MODERATE	VERY HIGH	HIGH	MODERATE	LOW
National Security - Internal	LOW	HIGH	VERY HIGH	HIGH	LOW	LOW
National Security - External	N/A	MODERATE	HIGH	MODERATE	N/A or LOW	N/A
Overall Category	High	High	Very High	High	Moderate	Low

* Above categorisation is just an illustrative example. It is the responsibility of the Line Ministry/Department to arrive at appropriate categorisation of the attributes.

Annexure E – Level of Strategic Control

(Page 8/Para 5)

Level of Strategic Control	Mechanism for ensuring Strategic Control	Staffing of CTT/PAC
Low Level	• At least CTT shall have necessary knowledge and overall understanding of the Architecture and the design.	• Resources can be taken internally or contracted from outside.
Moderate Level	• At least CTT shall have understanding of architecture, and the design with knowledge of tools and methodologies used. • Project could be outsourced to a lead vendor with one or more sub-vendors to enable backup(s). • Data accessibility should be allowed to limited and vetted personnel from the vendors.	• Resources can be taken internally or deputed from Government Organization, like NIC, C-DAC etc. Resources can also be contracted from organizations, like NeGD, NISG etc.
High Level	• In addition to the understanding of architecture and the design with knowledge of tools and methodologies used, CTT should participate with outsourced vendor in design and development of the system. • Implementation and rollout of the system could be outsourced to multiple vendors. • Data should be supervised/managed by CTT/supported by Government body.	• Resources can be taken internally or deputed from Government Organization, like NIC, C-DAC etc. Resources can also be contracted from organizations, like NeGD, NISG etc. (for NISG with approval from CPeMT).
Very High Level	• CTT along with Government body supervise the vendor(s) or • Government body, like NIC, could be chosen for solution development. • Critical data to be managed internally by the Government Department.	• CTT should be manned by Government officials and only in special case shall be hired externally with approval form Empowered Committee.

Feedback

Your comments and feedback are welcome. Please send an email to Renu Budhiraja at renu@mit.gov.in, Bhushan Mohan at bmohan@negp.gov.in.