Chapter

5

Monitoring and Evaluation

Handbook on e-Governance Project Lifecycle (2012) of Government of India states that it is imperative for the organizations to monitor and track achievement of stated project objectives and benefits throughout the lifecycle of the project. The quality of monitoring has a major impact on the extent to which effectiveness, efficiency, asset safeguarding and data integrity objectives are achieved in a project environment. Governance ensures that stakeholder needs are evaluated to determine balanced and agreed-on project objectives; direction is set through prioritization; performance and compliance are monitored against agreed-on directions and objectives as depicted in **Chart 5.1**.
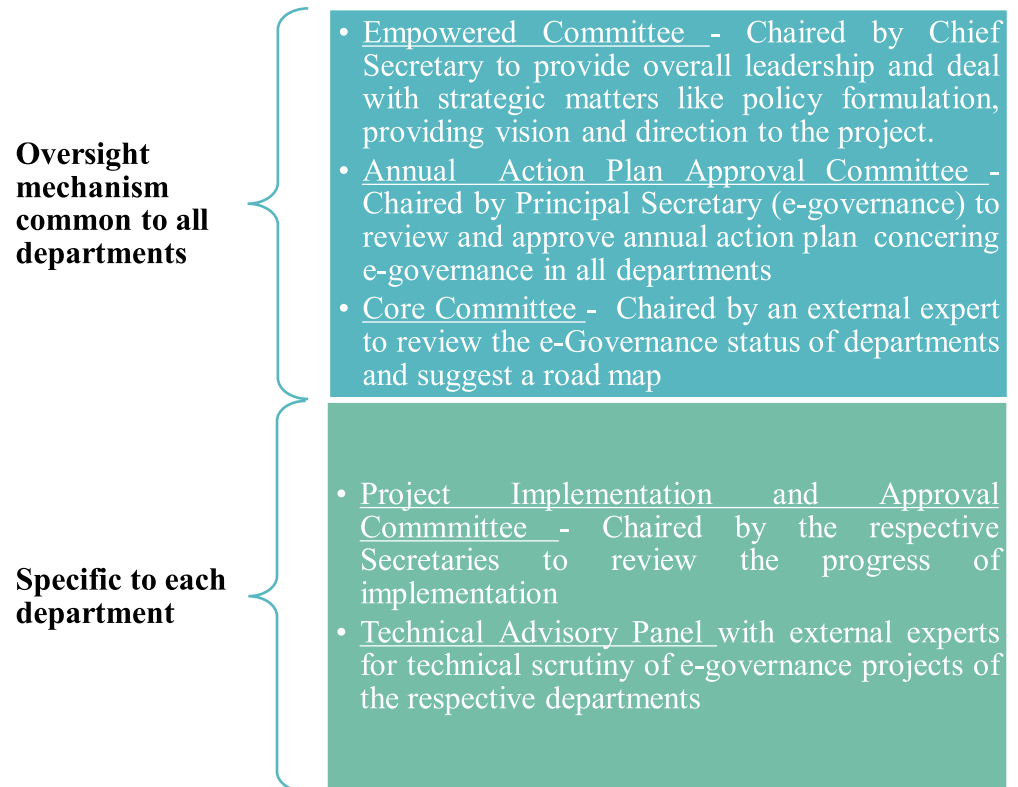
Chart 5.1: Governance of Information &Communication Technology
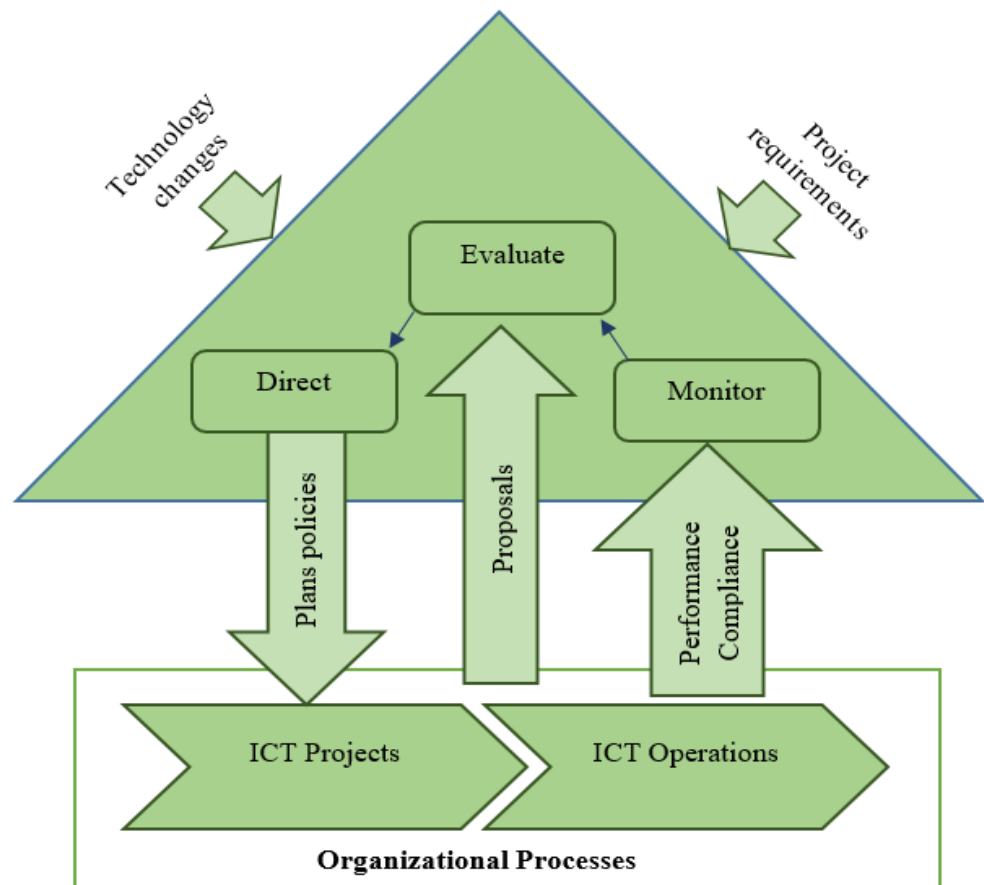
(Adopted from the ISO 38500 Model for Governance of IT)

5.1 Framework for IT Governance

Government of Karnataka had put in place an ecosystem for approval and monitoring of the e-Governance projects in Karnataka which included the following:

Oversight mechanism common to all departments

- Empowered Committee - Chaired by Chief Secretary to provide overall leadership and deal with strategic matters like policy formulation, providing vision and direction to the project.
- Annual Action Plan Approval Committee - Chaired by Principal Secretary (e-governance) to review and approve annual action plan concering e-governance in all departments
- Core Committee - Chaired by an external expert to review the e-Governance status of departments and suggest a road map

Specific to each department

- Project Implementation and Approval Commmittee - Chaired by the respective Secretaries to review the progress of implementation
- Technical Advisory Panel with external experts for technical scrutiny of e-governance projects of the respective departments

Further, in view of the functional and technical complexity of K2 project and its geographic coverage, the State Government constituted (October 2009) a Steering Committee (SC) to provide guidance and policy direction, address any inter-departmental and inter-agency coordination issues during project implementation and to accord approval to the deliverables. A Technical Committee (TC) was constituted (October 2009) to assist the SC and was responsible for providing high level technical guidance during project implementation besides reviewing the function and security compliance audit reports. Both these Committees were to interact with the SI on a periodic basis. As per the information furnished to Audit,

➢ The SC held 12 meetings during the eleven-year period (2010-2020) as against the requirement of one meeting per quarter.

➢ The TC met 25 times during the eleven-year period (2010-2020) period as against the requirement of one meeting per quarter.

➢ Only 3 TC and 1 SC meetings were conducted during the crucial period of 2012-2015 as all software development timelines including the project completion timeline were stipulated during this period.

The important deliverables to be approved by SC after review by TC and by TC after review by the PMU is shown below:

To be approved by SC	To be approved by TC
▪ Project Plan document ▪ Risk Assessment and Mitigation Document ▪ Change Management Plan ▪ IT Infrastructure sizing documents for primary and BCP/DR site ▪ Requirements Traceability Matrix ▪ Warranties and Licence Document	▪ Systems Requirement Study/Specifications Documents ▪ Detailed System Design Document ▪ Training Plan ▪ Standards Documentation ▪ Testing Approach and Plan Document ▪ Test Cases and Results ▪ Software & Hardware ▪ Digitized Records ▪ System Operations & Maintenance Manual ▪ User Manual

Audit observed that the SC and TC did not deliberate on the acceptance and approval of these deliverables by the SI in any of its meetings. Further, the procurement process and MSA required several important documents which required higher level consideration and technical approval as part of the project implementation. Scrutiny of the deliberations and minutes of the TC and SC meetings showed that the following documents were not considered and approved.

- ✓ Detailed Solution Technical Architecture
- ✓ Detailed Security Policy based on ISO 27001 standard
- ✓ Network Administration Policy
- ✓ System Administration Policy
- ✓ Exit Management Plan
- ✓ Data Migration Plan
- ✓ Communication Management Plan
- ✓ Incident Reporting Policy
- ✓ Backup and Recovery Policy
- ✓ Access Control Policy
- ✓ Preventive Maintenance Plan
- ✓ Quality Assurance Plan (as per IEE 730)
- ✓ Detailed Architecture Plan for DC& DR
- ✓ Pilot and Rollout execution Plan
- ✓ Upgrade path and plan for OEMs

In the absence of a specific approval by the designated committees, the documents submitted by the SI remain unauthenticated. Thus, the Governance framework established for overseeing the implementation of K2 was rendered ineffective, which led to prolonged delay in rolling out individual modules as discussed earlier and non-completion of the project even after a decade. Moreover, lack of a formal review and adoption by the committees charged with governance would undermine the credibility of these documents and their acceptance by the stakeholders.

5.2   Strategic Plan and Annual Action Plans not prepared

Taking into consideration the technological advancements, economic and social trends as well as the current and future organisational objectives that must be achieved, the DoT was expected to prepare a long-term strategic plan document indicating the strategies, proposals and supply arrangements, their evaluation and achievement monitoring together with the annual action plans which set forth the direction for providing funds for IT projects and operations.

The DoT did not furnish to audit any such documents which discusses the direction of the Department covering the IT aspects.

The Government stated (November 2021) that K2 evolved and incorporated all the latest technical advancements. Audit is of the view that long-term strategic plan document and annual action plan would facilitate orderly implementation of the e-Governance initiatives, in absence of which the incorporation of the technical advances will not materialize effectively.

The Government may ensure that K2 may consider preparing strategic plan to demonstrate and document the direction of the project that evolves with changing technology landscape.

5.3   Risk Management not documented

IT risk is a business risk specifically associated with the use, ownership, operation, involvement, influence and adoption of IT within the project. IT risk management is the process to continually identify, assess and reduce IT related risks within the levels of tolerance set by Project Executive Management.

The Information Security Management System (ISMS) Risk Assessment Methodology shared by the department provides for identifying and classifying assets, valuing the assets, analyzing the assets, estimating the expected loss due to risks and categorizing the risks. However, it was observed the process of identifying and classifying assets, valuing the assets, estimating expected loss due to risks was not undertaken. The risk register shared by the Department did not have the details of its approval and review by the Project Management.

The Government stated (November 2021) that the Department had initiated the process for internal audit for ISO 27001 certification and the agency engaged for the purpose shall develop an Enterprise Risk Management Framework and carry out risk assessment.

5.4   Performance indicators not specified and developed

Relevant Key Performance Indicators (KPIs) form the cornerstone of effective public sector performance reporting and are fundamental to public accountability. Audit observed that the Department had neither developed and adopted any performance indicators for monitoring the various activities of K2 project nor did it conduct any evaluation of the project during the implementation stage.

The Government stated (November 2021) that the KPIs were specified for the Treasury Department. Audit is of the view that the KPIs for monitoring the

performance of various activities of K2 such as user registration, recipient registration, reprocessing of failed payments, DSC renewal, accounting of receipts after receiving RBI scrolls, could be specified.

The Government may ensure that the Department prepare a catalogue of services offered by K2 to various stakeholders and specify KPIs and monitor the performance.

5.5   Project Evaluation

Project evaluation is the quality assurance mechanism that involve an assessment of a planned, ongoing, or completed programme to determine its relevance, efficiency, effectiveness, impact and sustainability.

Though the Project was closed from February 2019 and the department entered into a new O&M contract with the SI, no efforts were made to undertake a post completion evaluation of the project. It also failed to institute a mechanism to review the project to assess the achievement of planned objectives. Audit noticed that the SI continues its non-compliance even during the second contract such as delayed submission of the performance guarantee, non-setting up of the SLA measurement tools *etc*.

The Government stated (November 2021) that since the project was continued with the same vendor, the closure activities were not charted out. It also stated that the continuation of the second term has been conditional on the deliverables of first contract. The fact, however, remains that the deficiencies and learnings from the previous contract was not internalized and appropriate clauses to control the contract better were not used in the second contract. Therefore, the contractual lapses continued to occur and could derail the effective implementation of K2.