

INTERNATIONAL COOPERATION

tourist convenience

curriculum REFORM

Republic of Mauritius

GOVERNMENT PROCESS DEVELOPMENT TRAINING
NATIONAL ICT STRATEGIC PLAN

2007-2011

MEASURING THE INFORMATION ECONOMY
Broadband

emerging technologies, applications and standards

ELECTRONIC COMMUNICATIONS infrastructure

SECTORAL eGovernance

EVENT HOSTING

ict for social development

EXPLOITATION OF ICT

in the GDP HORIZONTAL TRANSFER

BUSINESS PROCESS OUTSOURCING TRAINING

information SECURITY

ICT EXPORTS

ICT Manpower

policy, regulatory and institutional framework

Development and Planning

public internet access points

local content

...now Scaling Up

ICT DOMESTIC

TECHNOLOGY TEST BED

ICT REGIONAL HUB

Multi-channel services



PART THREE

Structure of Part Three

This section details the institutional structure required for the ICT sector and is contained in two parts. The first part provides the “Implementation Framework” required to implement the programmes and projects recommended in this report as part of the NICTSP. The second part dwells on the “Institutional Framework” that is required for the ICT sector, and follows a scope review exercise earlier done during the “Analysis” phase of the project. The two parts have been covered independently of each other so that operationalising one of them is not dependent on the other’s successful completion.

Implementation Framework

A three-tier Implementation framework has been proposed with the tiers being (top-down) a High-Level Inter-Ministerial Committee(IMC) for the monitoring of the NICTSP, Programme Committees and Taskforces (PCTs) for implementing and monitoring the different programmes earlier described in the report and “owner” institutions that are separately and individually responsible for the implementation of the different projects. A secretariat to be attached to the IMC has also been suggested.

Terms of Reference have been outlined for the High-level Inter-Ministerial Committee, the Programme Committees and Taskforces (PCTs) and the Secretariat.

Institutional Framework

The Institutional Framework for the ICT sector is covered sequentially under the following broad headings,

- Functions that need to be performed for a growing ICT sector by a few identified bodies have been detailed;
- Lacunae earlier revealed during the “Analysis” phase gives a picture of where weaknesses in the current setup exist and hence provide indications as to what needs to be done;
- Critical Success Factors that at once become important for bodies in the ICT sector have also been covered, and, determined by these factors, recommendations have been made as to the type of body that must ultimately result; and
- Recommendations are then made that involve a two-step transition to the recommended “End State”, involving first a “Near Term Institutional Framework” before moving on to the “End State” of the National ICT Authority of Mauritius.

For both of these steps described above, the functions that need to be performed by the different institutions have been provided. For more clarity, the transition from the current state to the “End State” has also been diagrammatically illustrated.

Part Three Table of Contents

8	IMPLEMENTATION AND INSTITUTIONAL FRAMEWORK	149
8.1	IMPLEMENTATION FRAMEWORK FOR THE NICTSP	149
8.2	INSTITUTIONAL FRAMEWORK FOR THE ICT SECTOR	159

8. Implementation and Institutional Framework

The Importance of an Institutional Framework

An institutional framework is the quintessential vehicle used to implement government initiatives. Well-defined institutional structures become important for the following reasons.

- Institutional structures promise continued leadership, involvement and ownership of the initiatives that are planned and thus comfort implementers with a sense of continuity and commitment, be it from political or from the executive.
- They also make for clear ownership and accountability structures by detailing unambiguous roles and responsibilities for participating entities of the framework, even as they enable collaboration among them.
- Well-defined frameworks also ensure that the appropriate and compatible skill sets are deployed for the initiatives underway, while, at the same time providing adequate room for induction from outside.
- Institutional frameworks also have built into them proper monitoring and evaluating mechanisms which define terms under which a review of initiatives would be taken up and thus facilitate regular stock-taking of the progress achieved during implementation.

Recommendations for Institutional Structures in the NICTSP

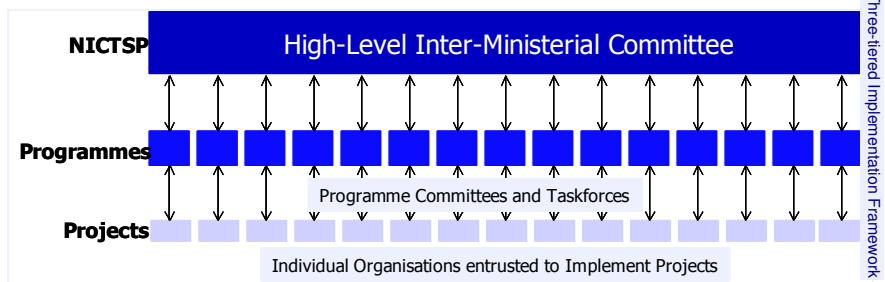
As part of the NICTSP, recommendations for institutional setups fall into two broad, relatively independent categories. They are as follows.

- A. Institutional structures required to implement and monitor the different initiatives (programmes, projects and recurring activities) under the NICTSP as covered severally under the programmes dealt with earlier; this is being referred to here as the IMPLEMENTATION FRAMEWORK.
- B. Institutional structure required within the government to fulfil its varied functions for the ICT sector. This, in fact, follows from a review of the scope of the organisational entities undertaken earlier during the analysis phase of the project, which has led to rationalisation of the activities being pursued by different bodies, and is being called the INSTITUTIONAL FRAMEWORK¹.

8.1 IMPLEMENTATION FRAMEWORK FOR THE NICTSP

A three-tiered implementation framework (Figure 16) is proposed for the implementation of the NICTSP programmes discussed earlier, comprising, bottom-upwards:

- **Project Execution and Monitoring:** As earlier discussed organisations have been identified that would take ownership of the different projects, with the team selection for the different projects being left to the different organisations themselves. The identified “owner” organisations for the different projects would be responsible for execution and monitoring of the individual projects.
- **Programme Execution and Monitoring:** A tier above is the programme implementation and monitoring which covers all projects that are associated with the programme. Programme Committees and Taskforces (PCTs)



¹ Since the INSTITUTIONAL FRAMEWORK would likely take some time to be effected fully, it is necessary that the IMPLEMENTATION FRAMEWORK for NICTSP be kept as independent of it as is possible. In other words, implementation of the NICTSP has been de-linked from the rationalisation process.

have been identified that are responsible separately for execution and monitoring the programme, including all the projects under it.

- NICTSP Monitoring: At the apex level, a High-Level Inter-Ministerial Committee (IMC) has been identified that will be responsible for monitoring the implementation of the whole of the NICTSP recommendations including the programmes that form a part of it. The IMC would be assisted in this with a Secretariat attached to it.

The following sections bring out a description of the functions to be performed at the three different levels.

1. The Inter-Ministerial Committee for NICTSP Implementation

However, at the apex level, there would be required a high-powered multi-stakeholder body, an Inter-Ministerial Committee to oversee and monitor the progress of the national Information and Communication Technologies Strategic Plan (2007-2011). The constitution of this body needs to have representation from the following stakeholder groups, at the minimum.

- a. the Ministry of Information Technology and Telecommunications (MITT)
- b. Ministry of Education and Human Resources (MoEHR)
- c. Ministry of Finance and Economic Development (MoFED)
- d. Ministry of Industry, Small and Medium Enterprises, Commerce and Cooperatives
- e. Ministry of Health and Quality of Life
- f. Ministry of Tourism, Leisure and External Communications
- g. Ministry of Agro-Industry and Fisheries
- h. Ministry of Labour, Industrial Relations and Employment
- i. the ICT Authority
- j. the National Computer Board
- k. ICT industry representatives, both domestic and export
- l. Academia
- m. Civil Society

Terms of Reference for the Inter-Ministerial Committee for Implementation of the NICTSP

The constitution of the Inter-Ministerial Committee for the implementation of the NICTSP (IMC) shall formally trigger the commencement of NICTSP. Through a group of meetings the IMC must formally adopt a Terms of Reference for itself in its role of rendering overseeing and monitoring functions for the plan.

The IMC must also decide upon a quorum (a minimum representation of its members) in any meeting where key decisions are taken.

An indicative Terms of Reference for the body is as follows.

The Inter-Ministerial Committee for the Implementation of the NICTSP (2007-2011) will be the single body at the apex level, chaired by the Ministry of Information Technology and Telecommunications (MITT), and with representation from other bodies as mentioned above, that would be responsible for monitoring and evaluating the implementation of the NICTSP.

Key functions the IMC would render are as follows.

Rolling out the NICTSP

- The IMC would collaboratively adopt its own Terms of Reference, and set up Committees/ Taskforces for implementation and monitoring of individual NICTSP programmes. The IMC would also roll out a General Terms of Reference for monitoring of individual NICTSP programmes which shall be adopted by the committees/taskforces.
- The IMC would collaboratively agree upon the timelines adopted and indicators with associated targets agreed upon by the Committees/Taskforces for their respective programmes. For this purpose the Committees/ Taskforces would submit their individual action plans, along with indicators and targets at least two weeks in advance of IMC's meeting for the purpose. This process would take place at the beginning of every year of the NICTSP implementation, except the first year, for which the Action Plan Report delivered as part of this consultancy would suffice.

Monitoring the NICTSP

- The IMC would convene a meeting of its members on at least a monthly basis to formally take stock of progress of the programmes whose implementation is underway. This process would be facilitated by implementation reports for the 15 programmes sent by respective Programme Committees and Taskforces (PCTs) at least a week in advance of the meeting of the IMC. The implementation reports must carry, at a minimum, the following information.
 - list of projects underway;
 - progress on the projects as measured by
 - adherence to timelines as adopted by the PCT;
 - self-evaluation of the projects by the PCTs in terms of indicators that were set out to measure the implementation progress;
 - reasons for slippage of time, if any;
 - measures proposed by the PCT to address the slippage;
 - ways in which indicators were measured or are proposed to be measured;
 - progress in terms of meeting targets associated with indicators;
 - reasons the PCT feels are responsible for any shortfall in meeting targets associated with indicators;
 - measures proposed by the PCT to bring about better performance on the indicators, if the targets associated with the indicators have not been met;
 - any other observations which the PCTs feels is important to highlight to the IMC.
- The IMC would take on board suggestions of the PCTs and evaluate the efficacy of the measures being proposed. Should the Committee think appropriate it would suggest changes in the PCT's approach.
- The IMC would also evaluate repercussions of any under-achievement in a programme (in terms of time, or otherwise) on any of the other programmes. Should it detect any such fallout, it would communicate the same to the affected programme's PCT and ask for concomitant changes to be introduced in the PCT's plans.

Endorsing and Communicating the Annual Budgetary Requirements

- Influenced by the above, the IMC would also endorse and communicate budgetary requirements for each of the succeeding years, with the first one having been completed through the Action Plan Report of this consultancy itself. This process would be facilitated by Annual Budgetary Requirement Reports for the 15 programmes sent by respective PCTs at least a month in advance of the meeting of the IMC in which this would be taken up.

Risk Mitigation

- The IMC would also need to take stock of any emerging risks and such other imminent possibilities that it thinks would significantly affect the smooth running of the NICTSP. The IMC, while addressing this issue would also come out with mitigation strategies to tackle such risks.

Inclusion/Exclusion/Amendment for the Projects

- The IMC would also need to deliberate on (a) the inclusion of any new project in any programme which it thinks has become important and therefore needs to be included, or (b) the deletion of any project which it thinks is no longer required or is no more feasible to implement, or (c) changing the contours of the project by taking into account any finding that was not known at the time the project was conceived. In all of these cases, the requisite changes would be made by the Committee/Taskforce in charge of overseeing the programme itself. Also, in all of these cases the IMC would fully take into account changes on account of inter-linkages between the different programmes.

NICTSP Representation

- The IMC would, on the basis of its meetings, also decide on representation aspects related to the NICTSP, be it to stakeholders in Mauritius or to audiences abroad. In drafting the content of such representation the IMC would be assisted by respective PCTs assigned for the individual programmes.
- The IMC would also be the sole authority to formally endorse all deliverables of the NICTSP that are for public circulation or amount to representing the country's interests. Indicatively, while the "State of the ICT Report" falls in the former category, the latter would typically be made up by draft Memoranda of Understanding with external agencies.

Facilitating Linkages and Finances

- The IMC would also facilitate linkages (a) among PCTs for different programmes on matters that demand collaborative working, and (b) facilitate linkage between one or more Committees/ Taskforces and any body that is outside the NICTSP implementation apparatus.
- Based on the budgetary requirements outlined in the Action Plan Report, the next deliverable of the project, and on any other considerations the IMC deems important, the IMC would ensure to make available to the respective PCT, the finances required to implement the programmes.

Any Other Matter

The IMC would take on board for deliberation and decision-making any other matter highlighted by the PCTs that demand its intervention. Conversely, the IMC would take into consideration all matters over and above the ones referred to above that it collectively decides to take up.

2. The Secretariat to the Inter-Ministerial Committee

Being a high-powered body with members drawn from various areas, the IMC may not be in a position to undertake the ground work required for the set of activities to be taken up. It is proposed, that, a 2-3 member Secretariat be also constituted who would do the necessary follow-up and coordination required to be undertaken for the purpose.

Brief Terms of Reference for the Secretariat is as follows

- The Secretariat to the IMC (SIMC) will be the single-body responsible for undertaking follow-up measures required upon decisions taken by the IMC, unless otherwise required and communicated by the IMC itself.
- The SIMC shall maintain written record of all minutes and deliberations at the IMC meetings for the NICTSP, and will be facilitated by an authorised email identification to help elicit and receive information on matters related to NICTSP.
- The SIMC shall function as the sole interface between the PCTs and the IMC for purposes of NICTSP.
- The SIMC will ensure that all implementation and budgetary requirement reports are obtained from PCTs requisite days in advance of the IMC's meeting. Should any delays arise the SIMC will accordingly schedule the meeting so as to give members of IMC adequate time required to go through the PCTs' deliverables.
- The SIMC will send out the formal invitation for the meeting of the IMC at least seven days in advance after due consultation with the members on their availability.
- The SIMC will collate all individual reports coming in from PCTs into a single document and highlight, where appropriate, action areas that demand attention from the IMC during its meeting. In such highlighting it will either use its own discretion, or work on general guidelines from the IMC or be informed by the PCTs.
- The SIMC will also ensure that all logistical arrangements are in place for the IMC meeting to run smoothly without interruption.
- For the Annual Budget Reports sent in from the PCTs, the SIMC will collate and highlight areas that represent deviation from what was originally planned in order to expedite proceedings during the IMC's meetings.
- Working under the IMC's directions, the SIMC will also undertake the required coordination efforts between the different PCTs and between members of the IMC itself.
- The SIMC will also undertake such other responsibilities which the IMC thinks are required and are of secretarial nature to facilitate smooth implementation of the NICTSP.

3. The Programme Committees and Taskforces (PCTs)

To implement the programmes (and the projects covered therein), taskforces and committees have been proposed separately under the different programmes earlier described in the report. The following is a brief Terms of Reference for the PCTs.

Terms of Reference for the Programme Committees and Taskforces (PCTs)

The constitution of the Programme Committees and Taskforces (PCTs) by the IMC for the implementation of the individual programmes under NICTSP shall formally trigger the commencement of the programme. The PCT will also adopt the Terms of Reference as laid out by the IMC.

The PCT will be the single body responsible for executing, monitoring and evaluating its programme.

Key functions the PCT would render are as follows

Rolling out the Programme

- The PCT would collaboratively decide on timelines to be adopted and the indicators with targets to be associated with the implementation of its programme. This process would take place at the commencement of every project that falls under the programme and at such other times that the PCT feels necessary. The PCT would convene a meeting for taking stock of the programme on a fortnightly basis.

Monitoring the Programme

- The PCT would collaboratively prepare and submit to the IMC Monthly Implementation Reports for its programme. The implementation reports must carry, at a minimum, the following information
 - list of projects underway;
 - progress on the projects as measured by
 - adherence to timelines as adopted by the PCT;
 - self-evaluation of the projects in terms of indicators that were set out to measure the implementation progress;
 - reasons for slippage of time, if any;
 - measures proposed by the PCT to address the slippage;
 - ways in which indicators were measured or are proposed to be measured;
 - progress in terms of meeting targets associated with indicators;
 - reasons the PCT feels are responsible for any shortfall in meeting targets associated with indicators;
 - measures proposed by the PCT to bring about better performance on the indicators, if the targets associated with the indicators have not been met; and
 - any other matter which the PCTs consider important to highlight.

Endorsing and Communicating the Annual Budgetary Requirements

- By at least a month in advance of the commencement of each of the NICTSP years, the PCT will ensure to have ready for submission the Annual Budgetary Requirement for the coming year. For the first year such a report already stands prepared in the Action Plan Report of this consultancy itself.

Risk Mitigation

- The PCT would also need to take stock of any emerging risks and such other imminent possibilities that it thinks would significantly affect the smooth running of the programme. The PCT, while addressing this issue would also suggest mitigation strategies to tackle such risks. Such risks should be included in its Monthly Implementation Report submissions to the IMC.

Inclusion/Exclusion/Amendment for the Projects

- The PCT would also need to advance suggestions on (a) the inclusion of any new project in any programme which it thinks has become important and therefore needs to be included, or (b) the deletion of any project which it thinks is no longer required or is no more feasible to implement, or (c) changing the contours of the project by taking into account any finding that was not known at the time the project was conceived. Again, such suggestions should be included in its Monthly Implementation Report submissions to the IMC.

Any Other Matter

- The PCT would also have within its scope any other matter highlighted by the IMC that the latter feels is required to be taken up.

Figure 17 brings out the institutional structure for the implementation of the NICTSP through a diagram.

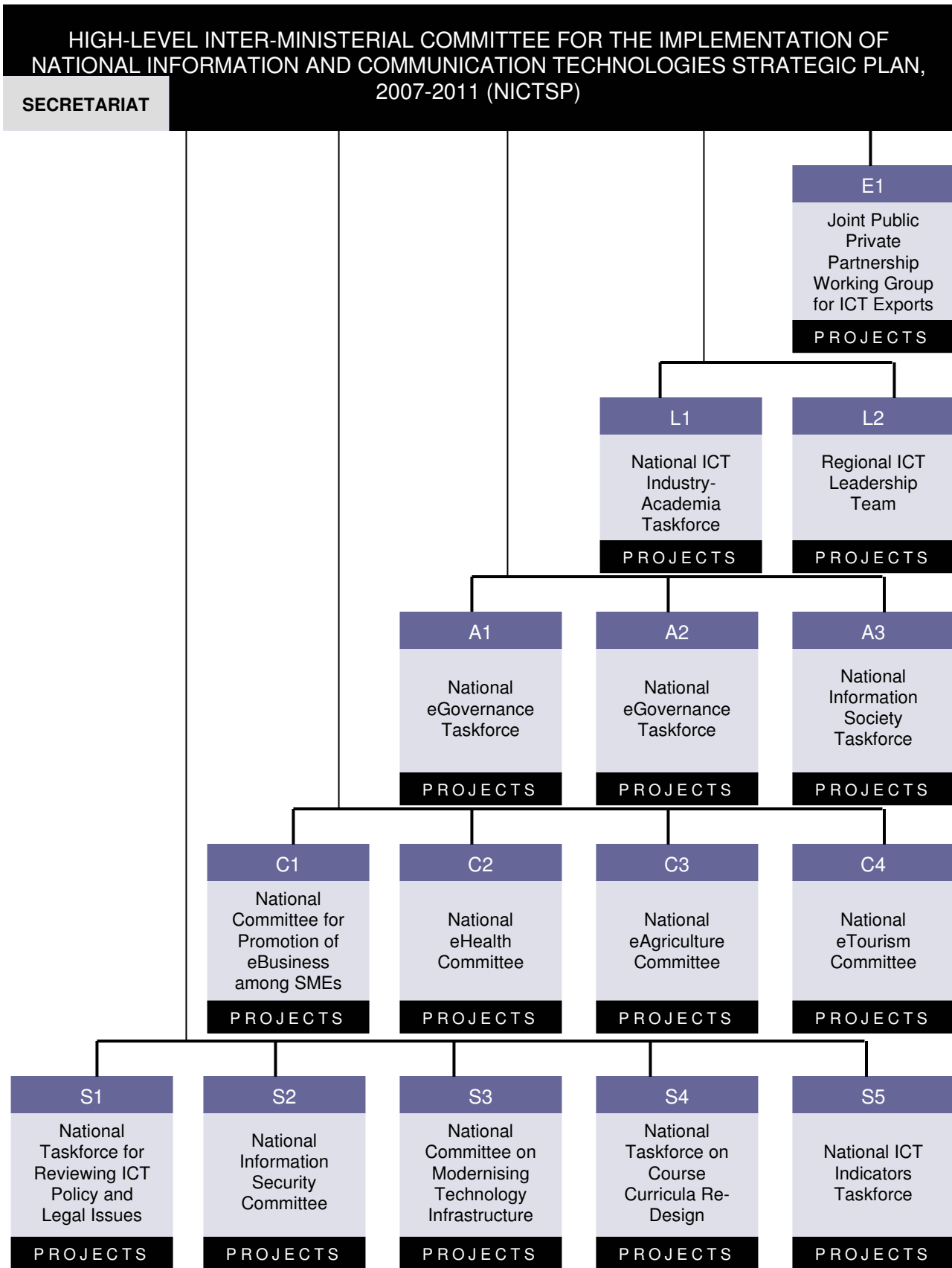


Figure 17 NICTSP Implementation Institutional Structure

The two tables over the next two pages (Tables 49 and 50) summarise the recommendations for the institutional structure required to implement the NICTSP programmes.

NICTSP level		PROGRAMME level	
		Programme Name	Programme Monitoring
High-Level Inter-Ministerial Committee to Monitor the Implementation of the NICTSP 2007-2011	SUPPORT	S1-FORMULATING AN ICT POLICY, EFFECTING LEGAL AND REGULATORY CHANGES	A National Taskforce on Revamping the ICT Legal and Regulatory Framework needs to be constituted, chaired by the MITT, including representatives from ICTA, State Law Office, HRDC, National Computer Board, ICT Industry Association.
		S2-INFORMATION SECURITY CULTURE AND EMERGENCY RESPONSE SYSTEMS	A National Information Security Committee needs to be constituted with representatives from the National Computer Board (chair), MITT, ICTA, MCCI, representatives from Critical Information Infrastructure areas, PMO, ITSU, a member from the Police Department, eGovernance Cell representative and a member representative of ISPs in Mauritius, to oversee and monitor the programme.
		S3- HARNESSING EMERGING TECHNOLOGIES AND ENHANCING INFRASTRUCTURE CAPABILITY	A National Committee on Modernising Technology Infrastructure Availability will be formed chaired by the MITT with representatives from MITT, ICTA, NCB, MT, ISP, IBA, ACT, MITIA, and business entities in the ICT sector, particularly those catering to export markets.
		S4- EDUCATION THROUGH ICT	A National Committee on Course Curricula Redesign for a Modern Workforce will be formed chaired by the MoEHR and will consist of representatives from MITT, MoEHR, MCA, MIE, NCB, TEC, UTM, UoM, IVTB, MQA, and representatives from other stakeholders. The committee will closely supervise and monitor the programme and, in case the work is awarded to an external consultancy, will serve as the Steering Committee for individual projects.
		S5-MAURITIUS ICT MEASUREMENT AND EVALUATION TERM REVIEW (MAURITIUS ICT METER)	A National ICT Indicator Taskforce (NICTIT) needs to be constituted with representatives from MITT (chair), Central Statistical Office, National Computer Board, ICT Advisory Council, members from ICT industry representing the ITs and the ITes sub-sectors, ICT Authority, and members from academia. MITT will chair the Taskforce.
	CATALYSE	C1- ENHANCE ICT UPTAKE AMONG SMES TO PROMOTE MARKET EXPANSION AND PRODUCTIVITY	An ICT in SMEs Committee chaired by the Ministry of Industries, SMEs, Commerce and Cooperatives (MISCC) and including representatives from Enterprise Mauritius, SEHDA, MITT, NCB, NVEC, SME Federation should be setup to drive and oversee the implementation and monitoring of the programme.
		C2- PROMOTING INTEGRATED ADOPTION OF ICTS TO DELIVER BETTER HEALTHCARE	A National eHealth Committee comprising representatives from Ministry of Health and Quality of Life (Chair), MITT, EGC, MIH, and from public and private sector health agencies to oversee and monitor the programme and serve as the Steering Committee for specific projects.
		C3- PROMOTING INTEGRATED ADOPTION OF ICTS THROUGH COLLABORATIVE WORKING	A National eAgriculture Committee chaired by the Ministry of Agro-industries and Fisheries and including representatives from MITT, EGC, Mauritius Chamber of Agriculture, and representatives of public sector and private sector stakeholders should be set up to drive and oversee the implementation and monitoring of the programme closely.
		C4- ENABLING INCLUSIVE GROWTH OF TOURISM INDUSTRY THROUGH ICT	A National eTourism Committee chaired by MoTL with representatives from MTPA, MITT, EGC, Tourism Authority, AHRIM, ASMH, Mobile operators, travel agents, car rental agency representative, representatives from the SMME sector in Tourism to oversee and monitor the programme closely.

ACCELERATE	A1- ACCELERATED E-GOVERNANCE THROUGH PROCESS RE-ENGINEERING AND COORDINATED PLANNING	A National eGovernance Taskforce chaired by the MITT and including Head of the eGovernance Cell, department heads of select departments, representatives from the business community, and representative of civil society groups, will be monitoring the progress of the programme closely.
	A2- UPSCALING E-GOVERNMENT THROUGH FLAGSHIP APPLICATIONS	A National eGovernance Taskforce constituted by the MITT, NCB, EGC, alongwith representatives from departments, ICT industry representative operational in the domestic sector, and representatives of civil society groups. MITT will chair the taskforce.
	A3- ENHANCING CONNECTIVITY AND CONTENT FOR COMMUNITY EMPOWERMENT	A National Information Society Taskforce constituted by representatives from MITT, NCB, ICTA, MT, UNDP, SEHDA, MACOSS, MoEHR, MoYS , and MPL would supervise the implementation of the programme. The taskforce will be monitoring the progress and also act as a Steering Committee if any of the projects is an external consultancy. NCB would chair the taskforce.
LEAD	L1- COLLABORATIVE PLANNING FOR MANPOWER DEVELOPMENT IN IT AND ITES/BPO SECTOR	A National ICT Industry-Academia Taskforce would be constituted by member representatives from Human Resources Development Council (HRDC), Ministry of Education and Human Resources (MoEHR), Ministry of Information Technology and Telecommunications, Tertiary Education Commission, Academia, the ICT Association, and member representatives from the ICT industry both from the domestic and the exports sector. The Taskforce will be chaired by the MoEHR.
	L2- BUILDING LEADERSHIP COMPETENCIES IN ICT	A Regional ICT Leadership Team to be constituted by member representatives from ICT Association, Board of Investment, ICTA, Ministry of Information Technology and Telecommunications (MITT), Ministry of Labour, Academia, National Computer Board, EGC and member representatives from the ICT industry both from the domestic and the exports sector. The team will be led by the MITT.
EMERGE	E1- A PREFERRED OFFSHORE DESTINATION FOR IT AND ITES-BPO SERVICES	A Joint Public Private Partnership Working Group to be constituted by member representatives from MITT (Chair), ICT Association, Board of Investment, Export Promotion Agency (as part of NCB), National Computer Board, and member representatives from the ICT industry primarily from the exports sector, will be monitoring the programme closely. MITT will lead the Working Group.

Table 1 NICTSP Implementation Institutional Framework

Representation Matrix for bodies required to implement NICTSP programmes discussed earlier is as follows. The cells marked red indicate the entity identified to take ownership of the programme, the letter “M” denotes the entity as a member representative in the Committee/Taskforce while the letter “C” indicates the entity as a chair of the Committee/Taskforce, while “F” in all cases denotes follow-up action by the Secretariat.

STAKEHOLDERS	INTER-MINISTERIAL TASKFORCE FOR NICTSP IMPLEMENTATION & MONITORING															
	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
SECRETARIAT																
MITT	C	M	M	M	C	M	M	M	M	C	C	M	M	C	C	
NCB	M	C	M	M	M	M				M	M	C	M	M	M	
ISPs		M	M													
ICTA	M	M	C		M							M				
EM						M										
BOI														M	M	
NGOs												M				
ICT Association													M	M	M	
Private Sector	M	M	M		M		M	M	M	M	M		M	M	M	
Academia				M	M							M	M	M		
HRDC	M			M									M			
IBA	M		M													
TEC				M									M			
Police		M														
eGovernance Cell*		M					M	M	M	M	M			M		
MoEHR				C									C	M		
MPL												M				
SLO	M															
Primary and Secondary Schools				M												
CSO					M											
NICTERN*					M											
MACOSS						M						M				
SEHDA						M						M				
MoTL									C							
MoAF								C								
MISCC						C										
MoHQL							C									
BPML			M													
NWEC						M										
SMEF						M										
Others			M				M	M	M	M	M	M	M		M	
	S1	S2	S3	S4	S5	C1	C2	C3	C4	A1	A2	A3	L1	L2	E1	

Table 2: NICTSP Institutional Responsibilities

8.2 INSTITUTIONAL FRAMEWORK for the ICT sector

This follows a scope review exercise undertaken during the Analysis phase of the project of a few identified organisations in the ICT sector. Concurrently, an exercise was also undertaken to understand the functions that need to be discharged by such organisations in a related country setting with comparable focus on the ICT sector as part of its larger economy. In this section, in light of findings of the above two exercises the following are covered.

- A Description of the functions that need to be discharged;
- Extracts from scope review undertaken during the “Analysis” phase of the project;
- Critical Success Factors that determine the type of organisation(s) that need(s) to exist for the ICT sector in Mauritius;
- Approach adopted for making recommendations on the Institutional Framework; and
- Recommendations for a gradual transition to the new institutional framework .

Functions to be Discharged

The spectrum of Functions to be performed by government agencies in the ICT sector are as covered in Figure 18.

Description of the Functions to be Discharged

In light of the comprehensive analysis done during our analysis stage, activities of the Institutional setup would involve the following functions

- Regulation and Enforcement, including activities related to regulating the activities of the ICT sector and enforcing the legal requirements as laid out in the statutes for the ICT sector.
- Promoting ICT Awareness and Adoption, including spreading the awareness of the need for and efficacy of ICT , and taking up initiatives that would encourage the adoption of ICT in the economy and in society at large.
- Educational Interventions, implying determining and recommending measures that need to be undertaken towards building up the manpower base for the ICT sector and to help internalize a “technology” temper in the society.
- ICT Statistical Operations, implying the monitoring and evaluation of various programme and projects being undertaken and employing statistical analyses to make recommendations on what needs to be taken up.
- Country Promotion and Investment, including taking up initiatives that would promote the country globally as a regional hub of activity as well as identifying markets for both the ITS and ITeS domains. This would also include undertaking activities to promote investments into the ICT sector both from within the country and beyond.
- eGovernance, implying using electronic means towards delivering good governance.
- Good eGovernance, implying the electronic enablement of and adherence to the principles of good governance as relevant for eGovernance.
- Technology Trends and Standards, implying keeping track of latest emerging technologies and standards, and ensuring their adherence and encouraging their adoption.
- Strategic Advisory and Policy Making, or extending inputs to the government in the required domains which would help GoM arrive at strategic plans and policies that would serve as guiding documents for stakeholders in the sector.
- Research and Innovation, which involves exploring and evolving new ways of discharging the above functions in a more efficient and cost-effective way for the collective benefit of the economy and society.
- Monitoring and Evaluation, implying activities related to undertaking periodical monitoring and evaluation of programmes and projects underway using objectively verifiable indicators.
- ICT Incubation, or promoting the growth of ICT businesses by offering incubation facilities to startups, including office space, basics technology infrastructure and other business support services.
- Information Security, including all activities related to building awareness and promoting adoption of Information Security and ensuring adherence to guidelines and best practices shared with the stakeholders from time to time.

Figure 18 Description of the Functions to be Discharged

Results of the Scope Review done during the Analysis Phase

Figure 19 brings out excerpts from the Analysis Report on the scope review done for organisations in the ICT sector attached to the MITT.

Excerpts from the Scope Review exercise executed during our Analysis Phase

- Agencies active in the ICT sector have ample overlap among them; there is noticeable duplication of efforts which may lead to ambiguity in execution and diseconomies of scale (for example, eGovernment activities are taken up by CIB, CISED and NCB). Similarly, ICT statistics are collected by NCB and ICTA, among entities attached to the MITT, and also by the CSO.
- Beyond ambiguity considerations, duplication of efforts may also lead to inappropriate competencies being used since the same skill set being required at many places, may not be available in full measure everywhere.
- For eGovernance operations, bodies like CIB, CISED, NCB etc are all MITT entities. The present institutional framework lacks representation from various other key ministries where eGovernance will actually take place. This may make for sub-optimal levels of ownership in eGovernance initiatives.
- Institutions analysed were originally created some specific mandates in late 80s and early 90s. However, even as they appear to have taken up activities that do not strictly lie within their assigned domains, no rationalisation has been done in the interim to define their activities more unambiguously. For example NCB was created to advise GOM on the formulation of national policies and legal framework for promotion and development of ICT and its application, has taken up activities in the sphere of eGovernment also.
- In the domain of ICT, a period of 15-20 years is a long one, and new activities and competencies have emerged that need to be considered. For example, BPO or the ITeS sector, or even off shoring, did not exist in significant measure when these Organisations were founded but constitutes a considerable share of revenue stream in ICT sector now.
- There is also no entity specifically entrusted with activities related to Research, Analysis and Innovation. Government needs to beef up efforts to disseminate information from its own research programs to trigger opportunities for innovation.
- There is lack of a coordinated mechanism to elicit feedback from citizens on how well eGovernance efforts are doing towards providing them convenience.
- For Mauritius to become a regional ICT hub, it is important for GoM to initiate strategic communications with other partnering nations. Although BOI is making efforts towards promoting investments into ICT, the need is felt for a more focussed agency that caters exclusively to ICT for attracting both business and investments into the sector from abroad.
- Although, going by the NCB Act, 1988, one of its objects for the Board is to undertake interventions in ICT education towards aligning it to industry requirements, NCB does not appear to be involved substantially in this area. However, though industry-academia exercises do happen, the need is felt for a more continual, comprehensive and collaborative approach facilitated by the MITT. MITT's involvement would ensure that initiatives that support such collaborative measures are in place, for example the necessary facilitation required for export promotion in order that targets set in industry-academia efforts succeed.

Figure 19 Excerpts from the earlier Scope Review done during the Analysis Phase

Critical Success Factors for the Institutional Framework

Keeping the observations of the Analysis Phase made during the scope review in the Analysis phase including the ones highlighted in Figure 19, the following Critical Success Factors are identified to be key to a successful implementation of initiatives in ICT sector, including those under the NICTSP.

- Political Leadership Involvement and Ownership, implying continued involvement, ownership, direction and support from the political leadership.
- Multi-stakeholder Involvement and Ownership, meaning continued involvement, ownership and commitment from government, private firms, academia, and civil society.
- Minimal Duplicity and Maximum Collaboration, or in other words, the revamped institutional setup must minimise duplication and maximise collaboration.

- Clear and Unambiguous mandate for the units/ Organisations, meaning that the institutional setup must be such as to facilitate clear and unambiguous roles and responsibilities of the constituent units/organisations.
- Compatible Employee Skillsets, or that employee skillsets available to be compatible with the mandate of their organisations.
- Minimum Professional Culture Shock, or that the rationalised institutional setup must minimise professional disruptions brought about by a radical change in work culture or by even more drastic requirements like downsizing of the workforce.
- Benefits of Synergy and Economies of Scale, implying that the new institutional setup must bring about economies of scale, minimise overheads, and facilitate synergistic networking.
- Easy and Quick Transition, or that the revamped institutional setup must be such as to enable easy and quick transition.
- Absorption and Induction of External Talent, implying that the revamped institutional setup must make for easy induction and absorption of professional talent and expertise from beyond what is currently available.
- Legal Flexibility, or that the institutional setup must be flexible enough to accommodate any changes through, if required, amendments to the very law under which the institution(s) has/have been set up. This, for example, is a key requirement in ICT where new skill sets may need to be inducted or organisations may need to get re-structured owing to developments in technology. Too rigid an institutional structure may not really make it amenable to such changes.
- Monitoring and Evaluation, meaning that the revamped institutional framework must facilitate a streamlined and closely monitored and evaluated implementation framework.

Approach followed for recommendation of an Institutional Framework

The Approach adopted for recommendation of an Institutional Framework is considered in two parts.

- PART ONE- The first part assess two alternatives. It assesses a multi-organisation setup for the ICT sector as against a unified single-body setup. The methodology followed for this is to evaluate how the two alternatives would fare when measured against the Critical Success factors discussed above. As the analysis below shows, a single-body setup is what must result.
- PART TWO- Given that there must be a single-body setup, the second part assesses different types of the single-body setup. Among the types considered are a Council, an Authority, a Board, a Public Limited Company that is government-owned and Public Limited Company that is owned by bodies outside the government. The methodology followed for this is also to evaluate how the five different options would fare when measured against the Critical Success factors discussed above. Again, as the analysis below shows, that a national-level authority is best suited to perform the functions identified with the unified single-body agency.

PART ONE

Table 51 brings out a comparison of the results of the assessment of the two alternatives

- A- Multi-Organisation setup for the ICT sector
- B- A Single Unified body for the ICT sector

Critical Success Factors	Alternative A- Multi-Organisation setup for the ICT sector	Alternative B- A Single Unified body for the ICT sector
Political Leadership Involvement and Ownership	Low to Medium , since political leadership may not be equally interested with equal vigour in all the Organisations. Organisations where the leadership is not as committed may lag	High , since it would be easier for the political leadership to be associated with one organisation. Also, being associated with one Organisation enables leadership to be more focused
Multi-stakeholder Involvement and Ownership	Low to Medium The same entity from outside the government may be required to become a part of different bodies. Entity may not be equally inclined to contribute fruitfully into ALL different ventures	High it is easier for the private firm to become associated and contribute into the same entity, Saves them time
Minimal Duplication and Maximum Collaboration	Low to medium , No matter how well the role allocation is done, there would always be ground for turf issues (duplicity factor). Initiatives often require multi-competency which would then reside in different organisations (collaboration factor).	High , All different competencies reside in one Organisation that has a single leadership. Even in the case of a contested piece of work, the leadership would always ensure that the same work is not being performed by two different units of the same organisation
Compatible Employee Skillsets	Medium Once rationalisation of Organisational mandate and re-deployment of staff is done, it would substantially increase employee compatibility	High , Different units will have their own mandates and they can select their staff accordingly. If ever a compatibility issue arises, it can conveniently be handled by a transfer from one unit to another.
Minimum Professional Culture Shock	Medium , No downsizing is expected to result in the new institutional framework vis-à-vis the old one. Incidence of culture shock is greater here for staff who shift from one organisation to another, following rationalisation of mandates	Medium , No downsizing expected to result in the new institutional framework vis-à-vis the old one. Incidence of culture shock is a little less here for staff who shift from their old organisation to the new entity, but under a common management
Benefits of Synergy and Economies of Scale	Low , Skill sets would be distributed in disparate organisations, each with its own overheads. Problems of coordination would arise whenever competencies that are distributed are required	High , Skill sets concentrated in the same single entity. Much less of coordination problems since essentially all skillsets are available under the same roof
Easy and Quick Transition	Medium , It would take some time for this transition to be made	Medium , It would take some time for this transition to be made
Absorption and Internalisation of External Talent	Low , Different organisations all well into their operations and attraction/retention of talents into a well-heelled setup will be difficult	High , People would be expecting change anyway. Discomfort arising out of the introduction of a new person at a key level will tend to get overlooked in the maze of other changes that are unfolding
Legal Flexibility	Low Difficult to effect changes in legislations for different organisations, with each of them requiring a sitting of the assembly	High Only one legislation needs be effected for the particular entity in question and this could be accomplished in one sitting of the assembly itself

Critical Success Factors	Alternative A- Multi-Organisation setup for the ICT sector	Alternative B- A Single Unified body for the ICT sector
Closely monitored and evaluated implementation	Low, Right now no M&E setup exists as such, and coming out with one may require substantial changes to be made	Medium, There being no M&E setup in the current framework, one needs to be created in the new framework; however, any discomfort arising out of this will tend to get overlooked

Table 3 NICTSP Organisational Possibility Assessment

It is apparent that Alternative B, where a single, cohesive organisation, is in charge of the complete spectrum of responsibilities, is the obvious answer that would help tide over most of the problems associated with the current institutional framework.

PART TWO- Type of Organisation in a Single Organisation Set Up

Five types of organisational entities have been considered

- a. Authority as a parastatal body established by an act of law, managed by a multi-stakeholder Board, chaired by top level political leadership, and legally empowered to regulate and enforce legal provisions.
- b. Council managed by a multi-stakeholder Board, led by the top political leadership, and entrusted with regulatory, coordination and promotional activities but not implementation.
- c. Board as a parastatal body, managed by a multi-stakeholder Board established by an Act and led by top political leadership performing the different functions associated with the ICT sector.
- d. A public limited company completely held by the government, with a management board that has representatives from the political leadership of the day at key positions, that performs the different functions associated with the ICT sector.
- e. A limited company that is profit-oriented and is completely privately held or jointly held by the government and the private sector, with an independent management board and entrusted with performance of different functions associated with the ICT sector.

Table 52 brings out how the five different organisational setups will fare on the different CSFs earlier discussed. As the figure illustrates the Authority as a parastatal body established by an act of law and managed by a multi-stakeholder Board, and chaired by the political leadership of the day is the most suitable option.

Table 4 Mauritius ICT setup- Assessment of Possibilities

Critical Success Factors Type of Single Unified Body	Political Leadership Involvement and Ownership	Multi-stakeholder Involvement and Ownership	Minimal Duplicity and Maximum Collaboration	Compatible Employee Skillsets	No Downsizing and Minimum Culture Shock	Benefits of Synergy and Economies of Scale	Easy and Quick Transition	Absorption and Internalisation of External Talent	People's Will and enforceability	Legal Flexibility	Closely monitored and evaluated implementation
	Authority established by an act of law, & legally empowered to regulate/enforce legal provisions	High	High	High	High	High	High	Medium	High	High	High
Council entrusted with regulatory, coordination and promotional activities but not implementation	High	Medium	Medium	Medium	High	Low	Medium	Low	Medium	Medium	High
Board performing the different functions associated with the ICT sector	High	High	High	High	High	High	High	High	Low	Medium	High
Public Limited Company completely held by the government & led by top political leadership	High	Low	High	High	High	High	Medium	Medium	Low	Low	Medium
Privately held company or jointly held enterprise in various combinations	Low	High	High	High	Low	High	High	High	Low	Medium	High

■ Low Suitability
 ■ Medium Suitability
 ■ High Suitability

Details of the Analysis

Of the five options considered above, the one of a “Privately held company” is ruled out owing to its poor ranking on the parameters of “Political Leadership”, “Culture Shock” and “People’s Will”. Being a profit-driven entity, it would be poorly placed on all of these.

Similarly, a “Publicly held company” would not fare very well on multi-stakeholder representation at the management board level (civil society representation may languish, for example), on legal flexibility requirements and when it comes to enforcing people’s will by taking up interventions in which to fulfil larger social responsibility requirements.

The choice then essentially boils down to choosing between a Council, a Board and an Authority. Of the three it is only the Authority which scores reasonably well on all the counts. Whereas a Council may be more of a decision-making, promotion, advisory and regulatory body, it would not delve into execution issues.

A Board, which again is the result of an Act, is not normally a body which would take care of people’s will and enforceability requirements, which is a handicap the Authority is unlikely to suffer from. It is easier for authorities to promote, regulate, advise and enforce. Change in work culture, though, necessitated by a movement to either the Board or the Authority is likely to be similar.

Figure 20 Details of Comparison between entities

Recommendation

Given the current institutional setup, it may not be completely realistic to move to the single unified body stage, the “End State” at once. What may be more prudent is to undertake the transition more gradually keeping requirements of change management in mind.

It is recommended that the movement to the “End State” be done in two stages:

- STAGE ONE or the Near Term Institutional Framework, and
- STAGE TWO, or the “End State” Institutional Framework.

Details of this transition are as follows.

STAGE ONE, OR THE NEAR TERM INSTITUTIONAL FRAMEWORK

In this stage, the multi-body setup is retained with some rationalisation taking place towards a more coherent distribution of roles and responsibilities that what is currently the case. Table 53 brings out aspects of this rationalisation. The following are the key points.

The National Computer Board

- The National Computer Board (NCB) will be the main planning and advisory body in the different spheres of involvement of ICT. It will continue with its operations in the areas of ICT business incubation, event hosting, awareness creation etc. However, it would not be doing operations in the sphere of eGovernance for example like the running of the GoC etc.
- The NCB would perform functions in the following areas, and in doing so would be the only body performing these roles with no overlaps with any other entity, except in the sphere of regulation as explained below.
 - Strategic Advisory and Policy
 - Monitoring and Evaluation of initiatives implemented by NCB (whether as part of NICTSP, or outside it)
 - ICT Business Incubation
 - Information Security (all functions except those under ITSU which continues as earlier)
 - ICT Awareness Building and Adoption
 - ICT Statistical Operations and Analysis

The NCB, will take on some new functional areas for performance of its roles, and in doing so would be the only body performing these roles with no overlaps with any other entity. The new areas are the following.

- ICT Educational Interventions, constituted largely by the scope of work as defined under programmes “S4” and “L1”, in both of which NCB is a member
- Research, Innovation and Analysis, as constituted by NICTERN, referred to earlier in the report under the programme “S5”
- Country Promotion and Investment for ICT, including functions discussed earlier under the programme “E1”
- Technology Trends and Standards, to be associated with the NICTERN as part of the group’s research and analysis work.

Information Security and the CERT-MU

- NCB will be responsible for all awareness creation measures and advisory inputs in the sphere of Information Security

- Additionally NCB will also be responsible for convening meetings of the National Information Security Forum, with representatives from Critical Information Infrastructure areas, that would be providing advisory inputs from functional standpoints in the forum meetings
- The CERT-MU would take responsibility of all operational aspects of information security` and will be housed in the NCB to begin with. However, after the CERT-MU's operations stabilise, the same would be moved to the MITT where it would take charge additionally of Information Security Assurance matters including compliance with guidelines etc. In such capacity the CERT-MU would also have enforcement powers.
- The ITSU may exist as earlier.

The ICT Authority

- The ICT Authority continues with its role as the regulator and would extend advisory inputs only in the sphere of regulation of ICT. However, ICTA would be the only body that would extend advisory inputs in the sphere of regulation and its enforcement, in both of which it would take into full cognisance requirements emanating from developments in convergence.
- In so far as regulatory matters are concerned particularly in relation to telecommunications, ICTA would also continue to perform its functions for "Technology Trends and Standards" as described in Table 53.

eGovernance

Like in ICT regulation, all eGovernance matters, of planning and advisory nature, will now be concentrated and centralised in the eGovernance Cell (EGC) which would be stationed in the Ministry of Information Technology and Telecommunications. The EGC will be the only body performing these roles with no overlaps with any other entity.

- For project management and operations' functions, the EGC will now be completely responsible for operating the Government Online Centre. Other changes recommended to be introduced to render project management and implementation functions are as follows.
 - The project managers of CIB would be associated with and positioned in the respective departments where eGovernment applications are implemented; together with the eGovernance Cell, the project managers (now eGovernance Change Managers in their departments) will take responsibility of implementing eGovernance in their respective departments. They would not be changing their departments, except under extraordinary circumstances which the MITT could define.
 - The CISD staff would also be tied up in small bundles of 5-7 people each for individual departments and would work closely and report to the eGovernance Change Managers who have been positioned there.
 - The top management of the CIB and the CISD will now become a part of the EGC and will need to work together towards delivering eGovernance.
 - A separate exercise will need to be undertaken (already mentioned under the Project "S1P11") which would find out if they, the top management of the CIB and the CISD have the requisite skills required to plan, innovate and implement eGovernance in Mauritius. Outcome of the exercise, in so far as eGovernance is concerned, would be (a) recommending the total strength required for the eGovernance Cell, (b) complete Organisation Chart for the EGC, along with job descriptions for members of the EGC, (d) allocation of roles and responsibilities to top management of CIB/CISD in EGC, and (e) if required, following a study of EGC's mandate, recommending whether an external eGovernance expert would be required or not and in what position within the EGC hierarchy.

- A separate exercise involving HR consultants will be carried out to finalise the placement of CIB and CISD officers in the new eGovernance Cell (EGC) and e-Governance Change Managers organisational set up.

Table 5 Alternative A- Distribution of Responsibilities

Parameter	MITT ²	NCB	EGC	ITSU	ICTA
Strategic Advisory and Policy Formulation ³					
Regulation and Enforcement					
Good Governance through eGovernance					
Promoting ICT Awareness and Adoption					
Country Promotion for ICT and Promotion of ICT Investments					
Interventions in ICT Education and Education through ICT					
ICT Statistical Operations and Analysis					
eGovernance					
Technology Trends and Standards					
Research, Innovation and Analysis					
ICT Business Incubation					
Monitoring and Evaluation ⁴					
Information Security					

STAGE TWO, OR THE “END STATE” INSTITUTIONAL FRAMEWORK

The following are the key points of this alternative, with reference to the results from our analysis done earlier. There would be one body for the ICT sector, which as discussion above shows will be an “Authority”, the National ICT Authority of Mauritius (NICTAM), to take responsibility for all functions of the ICT sector except matters related to regulation which will continue to exist with the ICT Authority.

The following are the key points associated with this recommendation. Reference is also made to the organisation chart shown overleaf (Figure 21).

- NICTAM will have a multi-stakeholder representation in its management board comprising representatives from the private sector, academia (Public sector) and other public sector representatives. The management board would also have in its decision-making capacity the heads of the Strategic Business Units into which NICTAM would be divided
- The following are the Strategic Business Units (SBUs) that would constitute the Authority
 - SBU- Planning, Advisory and Research, which will consist of the following sub-units.
 - The National ICT Evaluation and Research Network (NICTERN), that continues as earlier and moves in from NCB
 - The Office of Strategic Advice and Policy, which would be constituted by the Planning, Research and Development Wing of the current NCB and would take charge of all matters related to Strategic Advice and Policy.
 - The Information Security Cell, which would be constituted by staff in NCB working on Information Security aspects of advisory and awareness creation, the ITSU⁵ (now in the MITT) and the

² MITT- Ministry of Information Technology and Telecommunications, Government of the Republic of Mauritius, NCB- National Computer Board, CIB-Central Informatics Bureau, CISD- Central Informatics Systems Division, EM- Enterprise Mauritius, MITT

³ As explained above, Strategic Advisory and Policy Formulation in the sphere of ICT regulation will continue to be provided by ICTA. Similarly, in the sphere of adherence to IT Security Guidelines ITSU will continue to extend its functions as earlier

⁴ All agencies covered here continue to perform their Monitoring and Evaluation (M&E) roles for their respective activities while the Secretariat to the IMC discussed earlier performs M&E functions in so far as they are related to NICTSP programmes and projects

- CERT-MU. Together they would take charge of all matters related to Information Security. The cell would also convene meetings of the NISF as earlier, and, being part of an Authority will have enforcement powers.
- The Monitoring and Evaluation Cell (M&E Cell) which would be responsible for continual monitoring and evaluation of all programmes and projects underway as part of strategic plans (the current and subsequent ones). The M&E Cell would be made up by the Secretariat to the IMC of NICTSP.
- SBU-Operations which would take responsibility of all functions associated with eGovernance Cell and which will be made up by the EGC itself.
 - SBU-Country Promotion and ICT Awareness which would take responsibility of all functions associated with spreading awareness of ICT adoption benefits, matters related to business incubation in ICT and general country promotional aspects related to ICT. The SBU will be constituted by the following units.
 - Centre for Incubation, to be completely responsible for all matters related to ICT Business Incubation, and will be made up by the ICT Incubator Centre moving in from NCB.
 - Country Promotion Cell, responsible for the promotion of Mauritius at regional and global levels in coordination with other public and private Organisations of the ICT sector and would be constituted primarily by the Business Development and Promotion Division of the current National Computer Board.
 - Awareness Building Unit, which will be responsible for all matters related to increasing the uptake of ICT in the country among businesses and society and will be constituted by the ICT Culture Promotion unit of the NCB.
 - The “Centre for Good Governance through eGovernance” will be operationalised as a new initiative to enforce the Code of Good Governance through eGovernance, and will be an independent body though reporting to the Chairperson of NICTAM.

⁵ Alternatively since ITSU renders its functions in the sphere of bringing about adherence to IT Security principles and guidelines related to IT Security for government officials, it could also move into the SBU “Operations” that is constituted by the eGovernance Cell.

NATIONAL ICT AUTHORITY OF MAURITIUS

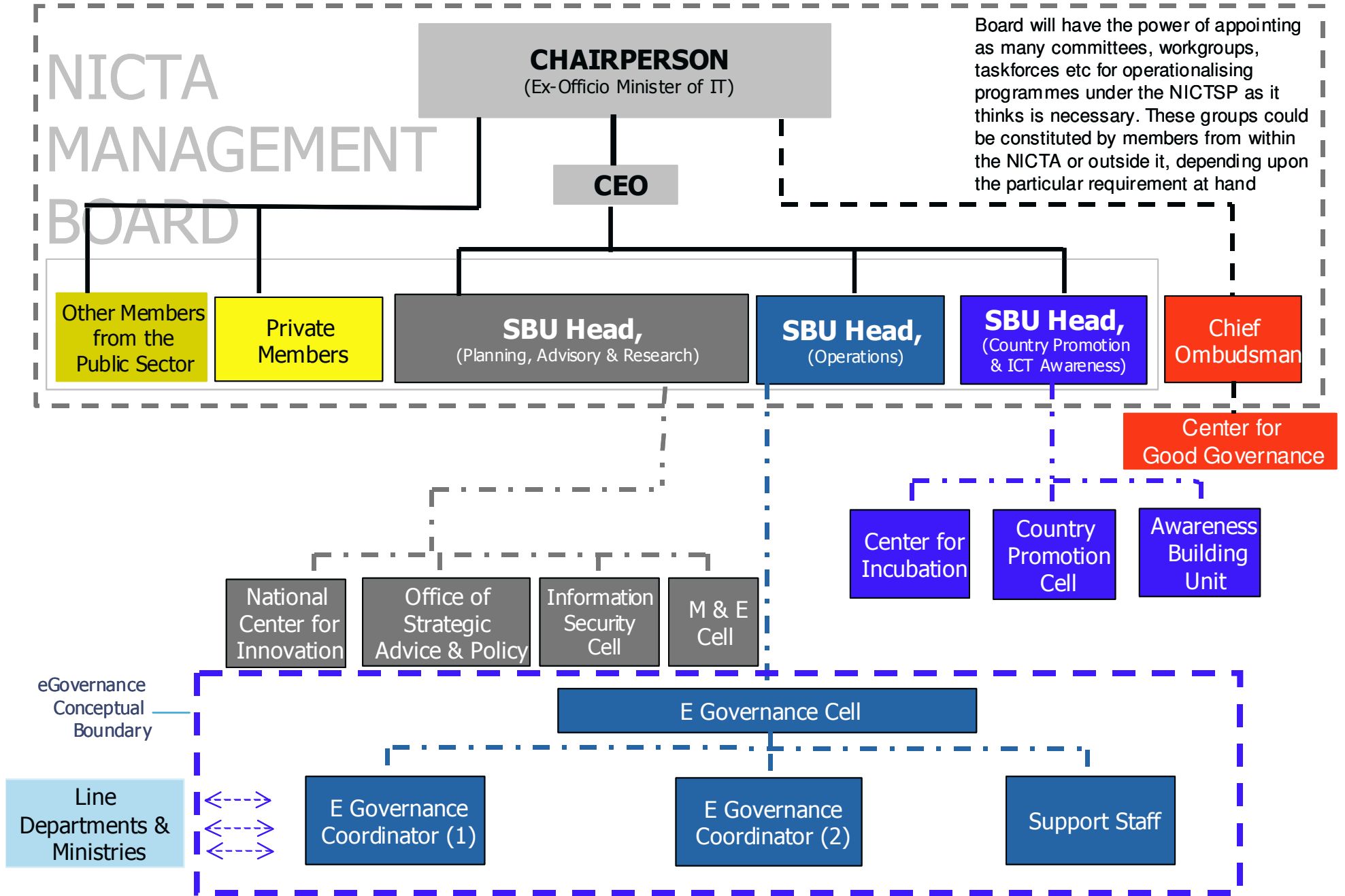


Figure 21 NICTAM Organisation Chart

Summarising and Illustrating the Transition from the Current Institutional Setup to the “End State” of NICTAM

Figure 22 captures essentials of what has been discussed above and illustrates the transition from the current state to the “end state” of the National ICT Authority of Mauritius as described above.

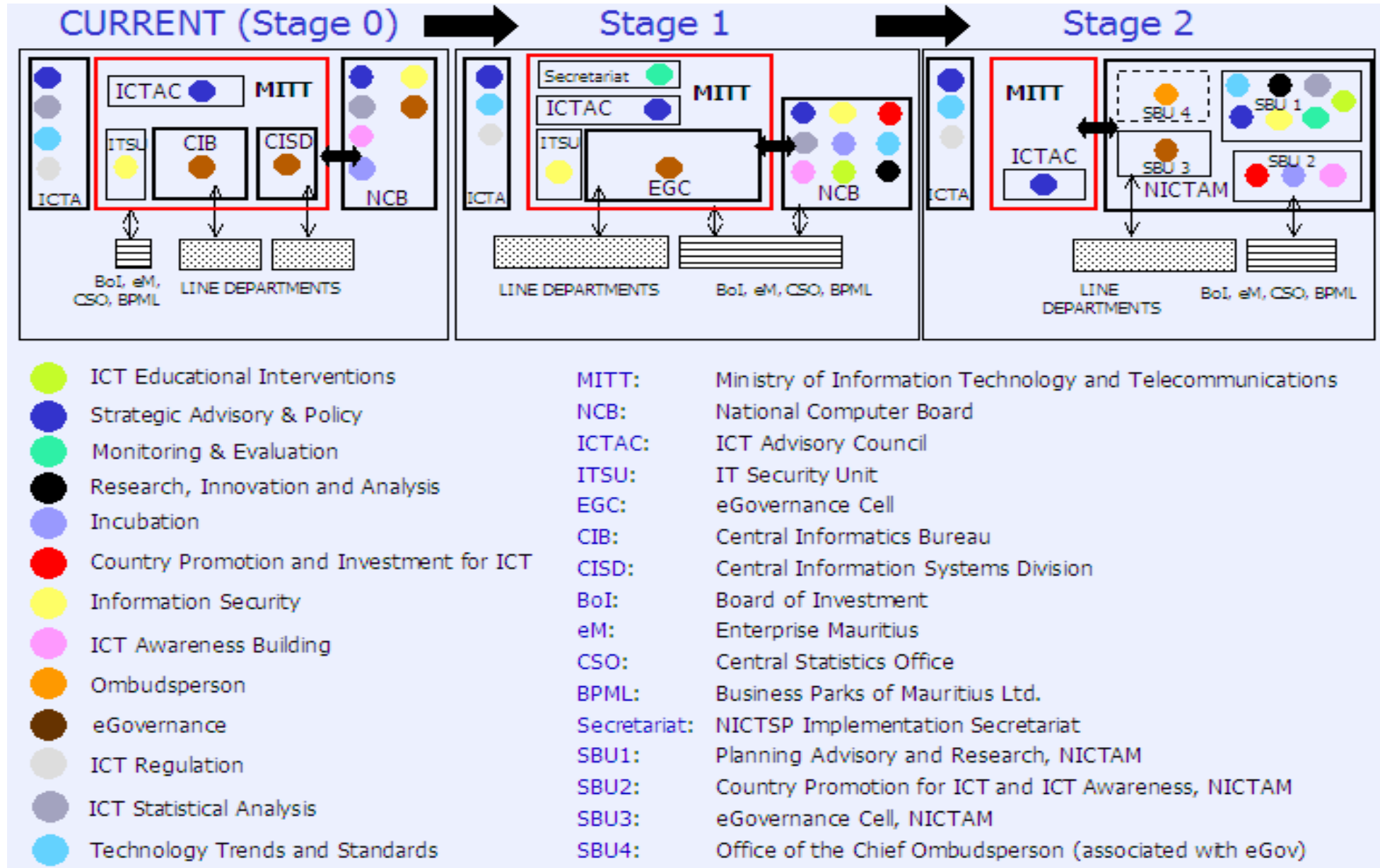


Figure 22 Transition from the Current State to the End State

The following constitute the salient points for the transition from

- (a) “Stage 0” to the “Stage 1”, and
- (b) “Stage 1” to the “End Stage” or the NICTAM

(a) “Stage 0” to the “Stage 1”

Key points associated with the transition are

The spectrum of functions to be rendered stand identified, as earlier described in Figure 21.

Bodies to deliver functions are uniquely identified

- The ICTA continues with its functions in the “Regulatory and Enforcement” domain. However, activities in the domain of ICT statistical analysis undertaken by the ICTA are now taken up by NCB. Modalities to effect this transfer are worked out.
- The NCB continues with its earlier functions, but adopts some new functional areas which it must take up, as described earlier.
- However, the NCB discontinues its functions in the area of eGovernance like the Government Online Centre and hands it over to the eGovernance Cell.
- An eGovernance Cell is constituted to lie in the MITT which would render all planning, advisory, monitoring and associated functions related to operationalising eGovernance in Mauritius.
- The CIB project managers move to their respective departments where they are stationed and are made responsible for implementation of eGovernance in their respective departments. A CIB project manager now becomes the eGovernance Change Manager in his/her respective department.
- The CISD staff also move in with project managers in bundles of 5-7 people and, together with eGovernance Change Manager become responsible for implementation of eGovernance in respective departments.
- The top management of both the CIB and the CISD now move in and together constitute the eGovernance Cell in the MITT. An exercise is undertaken to identify (a) the requisite skill sets required for the eGovernance Cell, (b) based on this drafting out Job Descriptions for the different members of the eGovernance Cell, and their reporting relationships etc, and (c) if, beyond the skillsets represented by the top management of the CIB and the CISD, any new skillsets are required, a decision is taken on either upskilling senior members of the CIB and CISD, or inducting new resources from outside. In other words, this exercise will result in the allocation of CIB and CISD personnel amongst the eGovernance Cell and the departments where eGovernance will be implemented. After this exercise, the EGC will stand completely defined.
- Both CIB and CISD cease to exist as earlier, and their top managements get merged to become the EGC, as discussed earlier.
- Since many of the new functions entrusted with the NCB do not fall as such in the mandate set out for it in the NCB Act, 1988, an exercise is undertaken to recommend amendments, if any to the said Act, including particularly the following domains
 - Information Security
 - ICT Statistical Operations and Analysis
 - Country Promotion and Investment for ICT
 - Technology Trends and Standards
 - Monitoring and Evaluation of the general efficacy of initiatives taken up in the ICT sector

(b) “Stage 1” to the “End Stage” or the NICTAM

- There is no impact on the ICTA

- The NCB as such as in “Stage 1” ceases to exist and, in its place, the National ICT Authority of Mauritius is formed with a much expanded role compared to what obtained for NCB in “Stage 1”
- The NICTAM is constituted by the four SBUs as defined earlier. A comprehensive Organisation Design with detailed Job Descriptions for officials of the NICTAM is worked out (Project “S1P11”). Necessary legislation required for this is also put in place.
- The NICTAM’s four SBUs are constituted by personnel sourced from bodies as described earlier.
- The eGovernance Cell merges into NICTAM.
- ITSU too merges into NICTAM as described earlier
- Necessary collaborative arrangements with entities like Bol and EM are worked out to make for streamlined operations.

9. Conclusion

As a successor to the earlier NITSP (1998-2005), the NICTSP (2007-2011) should be seen as a blend of reactive as well as proactive interventions towards influencing the socio-economic course of action for Mauritius. Though the seeds of the exercise were sown about 10 years ago, emerging economic realities in recent times decisively influence the recommendations made in the plan. They also threaten it with a sense of urgency.

The challenges for Mauritius in realising the ICT vision are manifold, and include,

- the constraint of a restricted supply of quality ICT manpower that would be the very fuel for an ICT-powered economy, not just in terms of the numbers in which they are available but also in the skill sets and abilities imbued in them through the educational process;
- sub-optimal levels of collaboration not just between sectors but also among entities in a sector itself, have not so far resulted in efforts being taken to their logical fruition; the results are often much less than what they could be;
- a steep cultural resistance to online transactions, owing primarily to ICT not having become a part of everyday life presents itself as a hurdle that needs to be surmounted, though in degrees; and
- a less than required acceptance of ICT not only as a career choice by the society but also as a stream at par with the other tracks of the economy is something that will need to be overcome.

Compounding the above challenges for Mauritius is the fact that, as an island nation, complexities it faces multiply even as the options available shrink. With the withdrawal of hitherto prevalent preferential trade regimes, the emergence of new and more competitive players in the international arena, and ICTs coming as a boon to some even as it threatens to leave many others behind, Mauritius cannot but look at ICT as a means to power its economy and take itself up the socio-economic ladder.

The SCALE framework gives us five broad strategic areas of thrust in which to pursue initiatives. The next deliverable, the Action Plan Report, supplies in detail the activities to be taken up within the framework of an actionable plan with loosely coupled interdependencies. As has been said earlier, if the holistic approach of the NICTSP strategy is its hallmark, a breach in adherence may well be a reason for the plan not doing as well as expected. Even as it is realised that getting the combined buy-in of all the stakeholders in the plan is not an easy task, every effort must be made to avert the possibility of the plan being implemented only in parts. Constructive collaboration is the main mantra and well coordinated and monitored efforts by stakeholders the chief instrument of delivery.

However, evolutionary, as against revolutionary, being the approach, the emerging situation needs to be visited as soon and as frequently as it may be affordable to discover emerging glitches, iron them out and identify new realities that surface.

10 Annexure I

ANNEXURE I : National Information Security Strategy

The National Information Security Strategy Plan (NISSP) is an important part of the Government's information society policy. Its main purpose will be to combat threats to information security. The NISSP will provide a common platform for the information security efforts of the Government, businesses, Organisations and individual citizens.

Information Security Concerns

The Information Society

Today's information society is epitomised by everyone now being able to send and receive vast quantities of information quickly, over great distances and at a low cost. At the same time, almost everyone can also access an infinite amount of information, knowledge and facts in a rapid manner. Rapid escalation in the level of e-business deployment leads to a multitude of electronic services currently available on the market today – and so far we have only scraped the tip of the iceberg in terms of developments within this area. The deployment of information technology has permeated almost every activity within society.

The risks are increasing in scope

Ubiquitous use of information technology has made society vulnerable within a variety of new areas. Malicious attacks on information systems can cause serious damage and disruption in normal services, e.g. in the form of unauthorised access, virus spreading and denial of service. Attacks can be mounted at any time, against anyone and from anywhere. In other words, society is facing completely new security challenges, the gravest of them being identifiable states' or factions' capabilities to organise and launch co-ordinated IT attacks with the intention of paralysing critical functions in a society. Beyond deliberate malicious attacks, vulnerability can also be attributable to inadvertent incidents – resulting from sheer carelessness or user ignorance. Vulnerability can also be increased by extreme weather conditions, such as floods and thunder storms, which also can have an effect on the scope of risk. Instability in information systems can also undermine confidence and thus inhibit widespread use of IT as a tool for creating new business opportunities.

Key challenges facing the information society

Identification of Critical Information Infrastructures

Information infrastructures can be described as critical if functionality of society, enterprises or individuals is severely affected by such a system's failure. It is imperative to identify these systems and gauge their position on a criticality scale. This is a prerequisite for risk assessments and implementation of critical protective measures. One distinct challenge here will involve identifying and securing infrastructures that are critical for the functioning of the society as a whole.

Securing critical IT infrastructures

Enterprises' security measures should be scaled according to an assessment of the identified risks. However, the challenge here will be to define a comprehensive set of generic criteria for securing critical functions in the society, partly because they differ so greatly. A generic set of common security measures will take care of the basic protection. Then, additional security measures at national, regional and local level can be implemented in particularly high-risk

situations. Security should include measures on physical, logical, and administrative levels. The development of suitable codes of best practice / standards in this area will undoubtedly pose a challenge.

Secure e-transactions

Far more extensive use of cryptography is recommended if in order to strengthen trust and confidence in electronic communication, e.g. to ensure that financial transactions are indeed secure and that private communications remain private. However, there is a potential drawback to private individuals or enterprises using advanced cryptography to protect their own information against unauthorised access, as this could obstruct police investigations into serious crime and cyber terrorism. These considerations must be weighed carefully against each other.

Drawing up regulations

National legislation, regulations and guidelines on information security have been developed over time and are based on a variety of needs. Many enterprises are obliged to follow several different types of regulations when they process many different kinds of information. It is therefore important to ensure that relevant regulations accommodate various security needs and take privacy into sufficient consideration. Development of new, and amendment of already existing, regulations shall be done in such a way as to make enforcement as easy and straightforward as possible.

Enterprises' focus on security

The management is primarily responsible for assuring an enterprise's assets, whether on behalf of society or the enterprise itself. The employees must be made aware of the substantial financial damage that could occur if there is a security breach. Large and middle-sized companies need to set up an in-house IT-security unit / task force with clearly defined responsibilities. The management ought to allocate adequate resources for security work. The companies without an in-house security unit / task force must see to it that the company commands enough skills to be able to assure adequate IT-security by engaging the services of external security experts. Security consequences of outsourcing of IT services need also to be evaluated. Clear lines of responsibility must exist for those implementing the IT-security measures and those auditing the actual implementation.

Emerging Security Risks

Increasing use of laptops, mobile phones and PDAs with Internet access are bringing new risks for businesses. Broadband technology enables IT equipment to stay "always on". Exchanging and synchronising data between portable and stationary units is becoming easier all the time. All this creates new challenges connected with uncontrolled information exchange and results in increased vulnerability and exposure to potential new types of attack.

A culture of security in society

We need to establish a culture of security in enterprises, public sector and the citizens, linked to the use of IT. A lot of users are not aware of the risks arising from using an information network. Many do not know of existing solutions for avoiding potential threats. This makes it difficult for an individual to assess the risks associated with Internet access. This also indicates a need to raise users' awareness of security threats and improve their skills in dealing with them. Safe use of the Internet has also an ethical dimension. This exacts new demands on acceptable ethical codes of conduct both on the part of Internet service providers and users themselves.

2. Principles of the National Information Security Strategy

The World Summit on Information Society Geneva Declaration of Principles states “strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs”. It further states that a “... global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies”.

The WSIS Action Line C5 recommends that member states implement measures along the following areas for Information Security:-

- Critical information infrastructure protection;
- Promotion of a global culture of cybersecurity;
- Harmonising national legal approaches, international legal coordination & enforcement;
- Countering spam;
- Developing watch, warning and incident response capabilities;
- Information sharing of national approaches, good practices and guidelines;
- Privacy, data and consumer protection.

The National Information Security Strategy is thus based on the WSIS Action Line C5 of the Geneva Declaration.

National Information Security Vision and Objectives

The National Information Security Strategy (NISS) is an important part of the Government’s ICT policy.

The vision for Information Security is aligned with the ICT vision is to “Transform Mauritius into an information-secure society, which supports the development of a trustworthy and competitive information economy”

The NISS will provide a common platform for the information security efforts of the Government, businesses, Organisations and individual citizens. The main goal of the NISS is to build trust and security in the use of ICTs.

The main objectives of the NISS are to:-

- Streamline and improve co-ordination on the implementation of information security measures at the national and international level;
- Protect critical information infrastructure from disruption through security breaches;
- Promote information security risk management and adoption of Information Security Standards at national level;
- Establish a framework for implementation of information assurance in critical sectors of the economy such as public utilities, telecommunications, transport, tourism, financial services, public sector, manufacturing and agriculture and developing a framework for managing information security risks at the national level;
- Establish an institutional framework that will be responsible for the monitoring of the information security situation at the national level, dissemination of advisories on latest information security alerts and management of information security risks at the national level including the reporting of information security breaches and incidents;
- Promote secure e-commerce and e-government services;
- Safeguard the privacy rights of individuals when using electronic communications and
- Improving awareness and competence in information security and sharing of best practices at the national level through the development of a culture of cyber security at national level.

National Information Security Strategy Measures

The measures of the NISS are based around the following areas of focus:-

- A. Information Security co-operation at national and international level
- B. Information Security Awareness and Education
- C. Trust and Confidentiality
- D. Information Security Risk Management
- E. Internet Governance
- F. Information Assurance

Information Security Cooperation at national and international level

The purpose of the National Information Security Strategy is to influence the creation of standards, policy guidelines and cooperation for promoting information security and to ensure that the division of responsibilities between the various actors in the field of information security is clear.

To this effect, it is proposed that a National Information Security Committee be set up under the aegis of the Ministry of IT and Telecommunications, including representatives from NCB, ICT Authority, operators of critical information infrastructure and regulatory bodies of other sectors to monitor the implementation of the measures of this Strategy, review and make proposals to update each regulatory authority's legislation impacting Information Security, propose clear cut guidelines for Information Security implementation in private sector and make proposals to Government for updating the Strategy after three to four years.

A working group will be set up reporting to the National Information Security Committee to provide status on information security and business continuity preparedness and national risk profiling on a regular basis. Operators of critical information infrastructure would also be represented in the working group. Closer collaboration with countries enjoying a more advanced culture of security will also be considered.

Information Security Awareness and Education

In a secure information society, everyone must be aware of the information security risks of their actions and of their responsibility in preventing these risks. The National Information Security Strategy is intended to raise the level of competence by investing in the expertise of information security professionals on one hand and in the general awareness of information security of all actors on the other.

All participants shall be made aware of potential threats, options, limitations and necessary action to advance establishment of a culture of IT security. The Government will promote awareness in this respect. All individuals are, however, responsible for obtaining necessary knowledge themselves, and to ensure compliance with the relevant legislation. Failure to gain essential knowledge could be detrimental to others, for which one could be held legally liable.

The following measures are proposed to this effect:-

- o Implement a National Information Security Awareness campaign targeting people in the workplace, public sector, students and general public to increase the awareness of individuals regarding information security issues by distributing factual information, producing info spots and incorporating information security education at all school levels. Distribute best practices for raising awareness to all educational institutions.
- o Review of curriculum for Computer Science and related subjects at Tertiary Level to include relevant information pertaining to needs of industry and businesses with regards to information security;

- Devise means for increasing number of professionals with Information Security Professional Qualifications (such as CISSP, CISA amongst others)
- Top management in private companies and public sector organisations are responsible to ensure their organisation have the necessary skills within Information Security based on well defined needs, and the organisation is committed to skills-promoting measures for its employees on Information Security.
- Suppliers of IT systems shall aim at transparency in informing customers with the level of security that their product can guarantee, under given circumstances. Suppliers should also follow internationally recognised security standards and provide support to users in the event of fault situations. Service Providers who place IT equipments and systems at the disposal of others should follow internationally recognised benchmarked security standards, defining security attributes as well as clarifying responsibilities held by the equipment's owner and its users
- Promote setting up of internationally recognised Information Security Association and local chapters of Internationally recognised bodies in the field
- Promote cooperation between industry and academia on knowledge sharing in information security areas through the holding of regular annual conferences on Information Security targeting major players and participants in the region.

Trust and Confidentiality

Building an information society with information security cannot happen at the expense of the fundamental rights and liberties of individuals and other actors. In a secure information society, all actors must be able to trust that their information and messages are processed and stored with confidentiality and will not be disclosed to unauthorised parties. Furthermore, everyone must have easy access to information for which they have authorisation.

To this end, the following measures will be implemented:

- The provisions under the Data Protection Act shall be implemented.
- Ensure that freedom of speech, confidentiality of communications, protection of privacy and other fundamental rights are taken into account in the legislation, official instructions and standards relating to information society services, electronic communications and information security, and in e-transactions services provided by public authorities;
- Establish a consultative process towards building a National Cryptography Policy;
- Implement appropriate mechanisms for the setting up of a Mauritian Public Key Infrastructure (PKI), including Controller of Certification Authority (CCA) for certifying local Certificate Authorities (CA). A Government PKI will be set up for the implementation of secure e-government services.

Information Security Risk Management

There is a need to provide greater transparency on how information security is handled in Organisations to improve trust and give comfort to users. In addition, monitoring of compliance to information security controls is done mainly at the level of the large organisations and Information Security standards has been adopted by the public and some large organisations mainly.

In Mauritius, there is no institution performing the role of a Computer Emergency Response Team (CERT) as is the case in other countries such as US, UK, India and Australia amongst others. To fight the increasing incidents of cybercrime, a vast majority of countries around the world have set up their own CERTs. The role of a CERT is to work with the Internet community to facilitate response to computer security incidents, to take proactive steps to raise the

community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. Moreover, in case of national disaster, the leadership responsible for measures related to preparedness and recovery for the national economy is not clear.

The following measures are proposed:-

- Set up a Mauritian CERT, (CERT-MU) for monitoring the national situation in information security risks, and constantly updated to provide timely information on the national situation to the major stakeholders CERT-MU will also be involved in activities such as Critical Information Infrastructure Protection and performing information security risk profiling and convey information on them and required counter-measures to all stakeholders. CERT-MU will be represented in the National Information Security Committee as well to provide status on the information security preparedness at national level.;
- A common set of criteria will be created to facilitate identification of critical IT infrastructures and systems. A method will be devised for risk and vulnerability assessments. The sectors will outline quality assurance standards for confidentiality, integrity and availability. The government will stimulate the development of security models, tools and mechanisms for risk analysis in order to encourage more efficient and user-friendly handling of IT security implementation.
- Security categorisation of information and security standards for private companies information processing should be adopted as far as possible.
- Information Security standards will be implemented in the Civil Service and parastatal organisations.
- Set up a working group responsible for identifying and monitoring critical information infrastructure protection under the National Information Security Committee.
- Set up a framework for monitoring Internet traffic which might be harmful to the nation and society;
- Promote the adoption and compliance to Information Security standards across the critical sectors of the society including SMEs.

Internet Governance

The main components under the WSIS Action Line C5 for Security issues of Internet Governance pertain to the problem of spamming, new forms of cyber crimes such as phishing, and safety of children online.

The measures to this effect are as follows:-

- Implement the recommendations of the Anti-Spam Action Plan;
- Enact appropriate legislations to counter the problem of spamming, new forms of cybercrimes such as phishing and to protect children online.
- Develop a Child Safety Action Plan, which will provide a roadmap for the protection of children and consumers online.

Information Assurance

Current status shows that, in few sectors, there is a reasonable number of documented policies and processes on information security. However there is a noticeable lack of monitoring of its compliance. In sectors, like, banking and financial sector, where there is a regime of strict and mandatory compliance, assurance activities on Information Security compliances are carried as per the requirement.

There is a unanimous concern that mandatory compliance and assurance processes would be a harsh financial burden on SMEs or small organisations. International Information Security standards could be tailored to reduce this

burden. Moreover, in the initial stages, only critical sector organisations be targeted for a mandatory Information Assurance which would subsequently widened to all organisations after a specific timeframe.

Thus the broad objectives of this area of focus would be to:

- a. Ensure that procedures and information security controls in place and are complied with.
- b. Provide a high degree of confidence the appropriate security controls are being effectively put in place for critical information infrastructure, which would minimise any disruptions in case of security breaches.

It is proposed to adopt the National Information Security Assurance Framework similar to the one implemented in India. To meet the above objectives, the following measures will be implemented:

- Promote the adoption of Information Security Standards at the National Level.
- Develop and implement a National Information Security Assurance Program (NISAP) for the public sector and for Organisation operation Critical Information Infrastructure. The salient features of this programme will be as follows:-
 - Government and critical infrastructure organisations (public or private) must have a security policy and nominate a point of contact;
 - Mandatory requirement for organisations to implement security controls and report security incidents to CERT-MU;
 - CERT-MU will create and maintain a panel of auditors of IT security, including penetrations testing and vulnerability assessment;
 - All organisations must be subject to third party audit from the panel once a year and whenever major configurations change; and
 - Security compliance to be reported to CERT-MU on a periodic basis

11. List of Abbreviations

AHRIM	Association hôteliers et restaurateurs de L'île Maurice
ASMH	Association of Small and Medium sized Hotels
BOI	Board of Investment Mauritius
BPML	Business Parks of Mauritius Ltd
BPO	Business Process Outsourcing
CCA	Controller of Certification Authorities
CERT	Computer Emergency Response Team
CIB	Central Informatics Bureau
CISD	Central Informatics Systems Division
COMESA	Commonwealth of Middle, East and Southern African States
COTS	Commercial Off the Shelf
CSO	Central Statistics Office
DBM	Development Bank of Mauritius
DOI	Digital Opportunity Index
DPC	Data Protection Commissioner
EGC	eGovernance Cell
EID	Electronic Identification Systems
EM	Enterprise Mauritius
ETA	Electronic Transactions Act
EU	European Union
GoM	Government of Mauritius
GPS	Global Positioning System
HORTIS	Horizontal Transfer of Indigenous Solutions
HRDC	Human Resource Development Council
IBA	Independent Broadcasting Authority
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Authority
ICTAC	Information and Communication Technology Advisory Council
IMC	Inter-Ministerial Committee for the Implementation and Monitoring of the NICTSP
IS	Information Security
ISP	Internet Service Provider
ITES	Information Technology Enabled Service
ITS	Information Technology Service
ITSU	Information Technology Security Unit
MACOSS	Mauritius Council of Social Services
MAGRIS	Mauritius Agricultural Resource Information System
MDG	Millennium Development Goals
MISCC	Ministry of Industries, SMEs, Commerce and Cooperatives
MITIA	Mauritius IT Industry Association
MITT	Ministry of Information Technology and Telecommunications
MoAC	Ministry of Arts and Culture
MoAF	Ministry of Agro-Industry and Fisheries
MoEHR	Ministry of Education and Human Resources
MoHQL	Ministry of Health and Quality of Life
MoLIRE	Ministry of Labour, Industrial Relations and Employment
MOST	Mauritius Offshore Services Team
MoTL	Ministry of Tourism and Leisure
MoWRCDPC	Ministry of Women's Rights, Child Development and Consumer Protection
MPL	Mauritius Posts Ltd
MQA	Mauritius Qualifications Authority
MT	Mauritius Telecom
MTPA	Mauritius Tourism Promotion Authority
NCB	National Computer Board

NGN	Next Generation Network
NGO	Non-Governmental Organisation
NICTAM	National Information and Communication Technology Authority of Mauritius
NICTERN	National Information and Communication Technology Evaluation and Research Network
NICTSP	National Information and Communication Technology Strategic Plan, 2007-2011
NRI	Network Readiness Index
NWEC	National Women Entrepreneur Council
OEM	Original Equipment Manufacturer
PCT	Programme Committee/ Taskforce
PIAP	Public Internet Access Point
PKI	Public Key Infrastructure
PoC	Proof of Concept (Prototype)
PPP	Public Private Partnership
RFID	Radio Frequency identification Device
RFP	Request for Proposal
SADC	South African Development Community
SBU	Strategic Business Unit
SEHDA	Small Enterprise and Handicrafts Development Authority
SIMC	Secretariat to the Inter Ministerial Committee for the NICTSP
SLA	Service Level Agreement
SLO	State Law Office Mauritius
SME	Small and Medium Enterprise
SMEF	Small and Medium Enterprises Federation
SMME	Small Medium and Micro Enterprise
TEC	Tertiary Education Commission
UNCITRAL	United Nations Convention on International Trade and Law
UNDP	United Nations Development Programme
UoM	University of Mauritius
UTM	University of Technology Mauritius
WWTE	Worldwide Travel Exchange

About the Exercise

The NICTSP was an extended collaborative exercise carried out from October 2006 to July 2007 involving ten Working Groups in the areas of ICT Domestic, ICT Exports, ICT Manpower Development and Planning, eGovernance, ICT for Social Development, ICT for Sectoral Exploitation, Information Security, Emerging Technologies Applications and Standards, Infrastructure and Electronic Communications, ICT Policy Regulatory and Institutional Framework.

PricewaterhouseCoopers India was the global consultant appointed for the exercise.

The exercise was supervised by the Technical Advisory Committee, chaired by the Chairman, National Computer Board, Mauritius and reviewed by a Steering Committee, chaired by the Hon'ble Minister, Ministry of Information Technology and Telecommunications, Government of the Republic of Mauritius, and co-chaired by the Country Head, United Nations Development Programme, Mauritius.

The exercise resulted in three main deliverables besides several working papers in the interim. The three main deliverables were

- The Final Analysis Report;
- The Strategic Framework Report; and
- The Action Plan Report.

NICTSP

2007-2011

