Report of the Technology Advisory Group for Unique Projects

Ministry of Finance
New Delhi, India

January 31, 2011

January 31, 2011

To,
Shri Pranab Mukherjee,
Honourable Minister of Finance,
Government of India.

Sir,

We submit herewith the Report of the Technology Advisory Group on Unique Projects (TAGUP).

Shri Nandan Nilekani
Chairman, UIDAI

Shri C.B. Bhave
Chairman, SEBI

Shri R. Chandrasekhar
Secretary, DoT

Shri Dhirendra Swarup
Former Chairman, PFRDA

Shri S.S. Khan
Former Member, CBDT

Shri P.R.V. Ramanan
Former Member, CBEC

Dr. Nachiket Mor
Chairman, IFMR Trust

Members

Chairman

Nandan Nilekani	Chairman, UIDAI

Members

C. B. Bhave	Chairman, SEBI
R. Chandrasekhar	Secretary, Department of Telecommunications
Dhirendra Swarup	Former Chairman, PFRDA
S. S. Khan	Former Member, CBDT
P. R. V. Ramanan	Former Member, CBEC
Dr. Nachiket Mor	Chairman, IFMR Trust

Secretariat

Amal Pushp	Additional Director of Income Tax, CBDT, DoR
Krishnan Dharmarajan	Director, National e-Governance Division, DIT
Parama Sen	Director, DoE
Ravi Agarwal	Director of Income Tax (Systems), CBDT, DoR
Ritesh Kumar Singh	Private Secretary to Minister for Petroleum and Natural Gas
Ritvik Pandey	Deputy Secretary, DEA
Satyajit Suri	General Manager (Program Development and Management), NISG
Somya Dave	Additional Director General, CBEC, DoR
Srikar M.S.	Private Secretary to Chairman, UIDAI
Dr. Viral B. Shah	Manager, UIDAI

Preface

The Finance Minister in his Budget Speech of 2010–2011 had announced the setting up of a Technology Advisory Group for Unique Projects. Para 104 of the Budget speech reads as follows:

> **Technology Advisory Group for Unique Projects**
> **104.** *An effective tax administration and financial governance system calls for creation of IT projects which are reliable, secure and efficient. IT projects like Tax Information Network, New Pension Scheme, National Treasury Management Agency, Expenditure Information Network, Goods and Service Tax, are in different stages of roll out. To look into various technological and systemic issues, I propose to set up a Technology Advisory Group for Unique Projects under the Chairmanship of Shri Nandan Nilekani.*

In recent years, Government functioning in general and specific projects in particular have come to involve complex Information Technology (IT) system development. Five projects stand out:

1. Goods and Services Tax (GST)
2. Tax Information Network (TIN)
3. Expenditure Information Network (EIN)
4. National Treasury Management Agency (NTMA)
5. New Pension System (NPS)

In addition, there are numerous other settings in Government where IT systems are mission critical.

These five projects alone have immense transformative power and can change India's growth trajectory. This justifies efforts in increasing the probability of project success. The challenge is to find ways to rapidly roll out these complex systems, to achieve project objectives and sustain high levels of reliable performance. Issues of project management for complex IT-intensive systems in Government need to be addressed on a priority. This report is an effort in this direction.

The Group held consultations with various experts within Government and outside. The consultations were held with Department of Economic Affairs, Department of Expenditure, Department of Revenue, PFRDA, CGA, CBDT, CBEC, NIC, CRIS, NSDL, NPCI, NASSCOM, and representatives of various State Governments.

Although the primary audience of this report are decision makers and the management teams of projects such as GST, TIN, EIN, NTMA, and NPS, the Group believes that

the framework put forth in this report is more generally applicable to the complex IT-intensive systems which are increasingly coming to prominence in the craft of Indian public administration.

The Group also recognises that various existing IT-intensive projects in Government are at different stages of implementation and with differing models. The adoption of the key recommendations of the Group to such projects should be done in a way that ensures minimal disruption to existing functioning.

List of abbreviations

BPR	Business Process Re-engineering
CBDT	Central Board of Direct Taxes
CBEC	Central Board of Excise and Customs
CVC	Central Vigilance Commission
DEA	Department of Economic Affairs
DIT	Department of Information Technology
DoR	Department of Revenue
DoE	Department of Expenditure
DoT	Department of Telecommunications
EIN	Expenditure Information Network
GFR	General Financial Rules
GOI	Government of India
GST	Goods and Services Tax
GSTN	Goods and Services Tax Network
IT	Information Technology
ITD	Income Tax Department
KYC	Know Your Customer
MoU	Memorum of Understanding
MSP	Managed Services Provider
NISG	National Institute for Smart Government
NPCI	National Payments Corporation of India
NPS	New Pension System
NSDL	National Securities Depository Limited
NSE	National Stock Exchange
NTMA	National Treasury Management Authority
NIU	National Information Utility
PAN	Permanent Account Number
PFRDA	Pension Fund Regulatory and Development Authority
RFP	Request for Proposal
RTI	Right to Information
SEBI	Securities and Exchange Board of India
SLA	Service Level Agreement
TAGUP	Technology Advisory Group for Unique Projects
TIN	Tax Information Network
UIDAI	Unique Identification Authority of India

Executive summary

In the last two decades, the Government of India (GOI) and many State Governments have initiated several e-Governance projects many of which have brought about significant changes in the way the concerned Departments and Agencies had conducted their business in the past.

The Finance Ministry in the GOI has been in the forefront of such initiatives and has successfully implemented large, complex projects involving extensive use of IT Systems, such as the TIN for Income Tax applications, ICES for Customs, and ACES for Excise and Service Tax. Similarly, the vision of organized financial trading (stock exchanges, depositories, and clearing corporations) has been implemented successfully using IT systems through the joint efforts of various stakeholders.

Undoubtedly, all of them have to be built on sound and durable IT systems for better management. Considering the complex nature of these projects, it is necessary to not only get the design and implementation of such systems right, but it is also essential that institutional capacity be built up to support these projects and sustain them on an ongoing basis. The challenge is thus that of finding ways to rapidly roll out these systems, to achieve and then to sustain high levels of reliable performance on an ongoing basis.

The Group reviewed these five projects along various dimensions. The challenges faced in implementing ongoing projects like TIN ,ICES and ACES have been a valuable guide. The most important lesson that needs to be acted upon is that business change' should drive the design and implementation of these projects. IT is essentially an enabler and a powerful tool to achieve the expected business change. In this sense, IT is a means to an end.

In the course of these reviews, the Group observed similar patterns and challenges across all projects, and a common framework for evaluation evolved naturally. Thus, this report starts out by addressing the challenges faced by large complex IT projects in Government, and then applies this framework to the evaluation of the five projects at hand. Part I discusses the public policy challenges. Technology challenges are discussed in Part II. All projects are then evaluated within this framework in Part III.

Public policy challenges

Chapter 1 analyzes the first of the public policy challenges, namely, the appropriate placement of tasks. IT projects in Government, if small, are typically implemented in-house, and if large, or contracted out to Managed Service Providers (MSP) or vendors. Taking into account the complex nature of 5 projects in view, and the

project management challenges, the adoption of a National Information Utility (NIU) framework , where the Government focuses on policy formulation and enforcement, and the NIU on implementation of IT systems to enable the proposed business changes is recommended. Besides, the recommendations cover the aspects of ownership and governance structure of the NIU, strategic control by the Government, and allocation of responsibilities between the Government and the NIU.

Considering the importance of investment in *peopleware* in the successful implementation of complex projects and the need to nurture talent to sustain continuous improvement, Chapter 2 discusses the second challenge, namely, human resource issues. The recommendations herein cover aspects such as setting up of a dedicated Mission Team headed by Mission Leader, a five year tenure for the team to ensure continuity, revising Deputation schemes within Government, induction of talent from outside the Government,wider use of contractual appointments, capacity building through induction and advanced training programs,grant of incentives to retain in-service officers on projects, creation of conducive work environment and improving methods of performance appraisal methods, especially for personnel appointed to key projects. Similarly, the NIU must also have a dedicated management team that mirrors the team within Government.

Chapter 3 discusses the issues that are relevant for giving shape to the contractual relationship between the Government and the NIU in a vendor-customer mode. In line with the recommendations for the adoption of NIU framework, wherein NIUs will work in the spirit of partnership with the Government, detailed recommendations have been made on the aspects to be touched in the agreement with NIU, such as scope of work,activities to undertaken by the NIU, financial arrangement, obligations of the NIU and the Government, SLAs, and business continuity plan upon exit.

The challenges faced by projects from startup to going concern are addressed in Chapter 4. The needs of a project in the startup phase are quite different from its needs in steady State. These may vary from mundane issues such as office space, to complex issues such as legal frameworks and bringing all stakeholders on board. The recommendations focus therefore on issues such as, incubation process before the NIU comes into being, need to set up dedicated teams within the Government as well as the NIU, need for consultations with stakeholders, preparation of a Mission Strategy Document, rapid roll out based on the experience of pilots and the relationship during the start-up phase.

Chapter 5 discusses specific challenges faced by projects that span multiple levels of Government. The Group is of the view that the seemingly opposite characteristics of federal, decentralized governance and the need for a unified approach through a single software application with common functionality can be resolved with the right solution architecture evolved through a process of consensus. Incentive compatible solutions for all levels of Government are necessary to bring about a coalition for change and ensure full participation and success for such projects.

Technology challenges

Chapter 6 points out some key design considerations for the solution architecture. The solution architecture should be designed to be flexible, reusable, extensible by stakeholders, and free of vendor lock-in. Given that many Government projects touch end-users such as citizens and firms, the Government should also play an active role in promoting banking and accessibility for all. This can form the basis of a platform for delivery of services.

Chapter 7 addresses openness in implementation of Government IT projects. It describes the relevance of open standards, open data, and open source. The Government

should not only be a consumer, but also strive to produce and facilitate open standards, open data, and open source. It also suggests the creation of an open source foundation for open sourcing software from Government projects.

Chapter 8 discusses security for systems of strategic importance. Today, attacks on IT systems are getting increasingly sophisticated. Systems such as those that are the focus of this report are likely to be targeted. Compromise may also happen from within the organization. Security must be taken seriously, and should be one of the topmost concerns of the management team.

Chapter 9 describes mechanisms of accountability and transparency that should be built into the design of IT systems in Government. Transparency cannot be an afterthought. It is essential to define what data will be released early on, so that the IT system can be architected accordingly.

Chapter 10 describes safeguards in technology and processes that should be built into the design of IT systems to protect the privacy of individuals. Privacy, like transparency cannot be an afterthought. Privacy and transparency are also not at odds with each other, and a well-planned system can easily achieve both.

Recommendations on Ministry of Finance projects

Chapter 11 discusses the strategy and implementation of the GST project. The recommendations, take note of the impending implementation of GST and cover the setting up of GST Network as an NIU, incubation of the project in NSDL, the need to set up a dedicated Mission Team on a priority basis, the placement of tasks in the NIU, the setting up of a continuing consultation process among the stakeholders, the broad features of the solution architecture of the GSTN, and the way forward from the pilot stage to steady state.

Chapter 12 discusses the working of the TIN project and the IT systems within the Income Tax Department for processing the information flowing from the TIN. The Group notes that with the impending operationalisation of the Direct Taxes Code, major changes in the application solutions are called for. The way forward would be to set up an NIU to design, develop and manage its IT related infrastructure on long-term basis and also to replace the existing application of diverse implementation methodologies. The recommendations to achieve project objectives have also been set out.

Chapter 13 discusses the Expenditure Information Network. The existing system of expenditure has some limitations. Today, measurement of plan implementation is on the basis of outlay rather than outcome. Government follows hierarchical and multiple patterns for allocation and release of funds to the implementing agencies and beneficiaries. It is difficult to track the flow of funds to actual beneficiaries, and equally difficult to evaluate the performance of agencies based on spending and project implementation. The Group recommends that a Mission Team be set up within Government along with an NIU for implementing the EIN. A high level solution architecture for the EIN is also described in this chapter.

Chapter 14 discusses the way forward for NTMA. It is seen that the Internal Working group on Debt Management (WG) has provided detailed steps for incubating the project, setting up of IT systems, the need for creation of databases on debts and contingent liabilities and change management for transferring the functions from RBI to NTMA. The Group commends the approach suggested by the WG, and recommends that an NIU approach be adopted for the implementation of IT systems for NTMA.

Chapter 15 discusses the status of IT systems set up to meet the requirements of the New Pension System. The suggested way forward is to work towards convergence of all pension and provident fund streams, rationalization of tax treatment of NPS to provide

more even treatment with other retirement products and providers and creation of awareness among the subscribers. Recommendations for implementation have also been indicated.

The report concludes with a summary of recommendations in Part IV.

Contents

Part I

Public policy challenges

1

The appropriate placement of tasks

1.1. Background

Over the years, several projects, both large and small, have been implemented in the Government sector in India with varying degrees of success. Some of these projects are yet to meet the expectations of the ultimate users as well as the departments that conceived these projects. While reasons for the same are many, one that has been a recurring theme in all the projects has been the inability of the concerned departments to implement and manage them efficiently and effectively in a sustained manner.

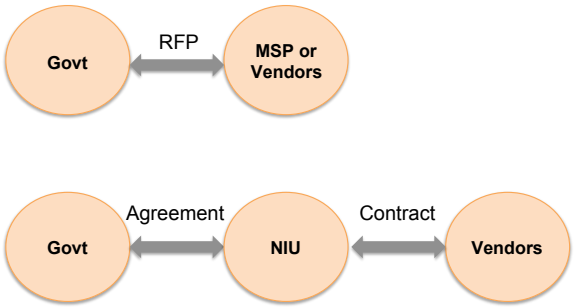
Typically, IT projects supporting Government functions are developed within Government for small projects, or outsourced to a Managed Services Provider (MSP) or one or more vendors for larger projects. In the MSP/vendor model, the Government Department puts a project team in place, which carefully studies the business requirements and writes a Request for Proposal (RFP). An MSP/vendor is then selected through a competitive bidding process. In the case of highly specialised projects, Government has also followed the route of selection of service providers on nomination basis after rigorous evaluation of alternatives and negotiation of price by an expert group consisting of resources from within and outside.

Invariably, managing such projects has been a great challenge. Often, the implementation team has had to face serious problems due to lack of financial independence, inability to get the right personnel and retain them, technological obsolescence, lack of speed and productivity in implementation, lack of ownership on the part of the user community within the department, leading to cost and time overruns and failure to fulfill the requirements.

The Group is of the view that for complex projects that depend on mission-critical IT systems, like the GST project, there is a clear need to move away from the above mentioned implementation models. A robust and flexible institutional framework, combined with a strong dedicated team is necessary to successfully implement such projects in Government. Alongside, appropriate placement of tasks and allocation of responsibilities as between the Government and the supporting institutions are essential to achieve the goals and objectives of the projects.

The Group recommends that a class of institutions called *National Information Utilities (NIU)* may be put in place to handle all aspects of IT systems for such complex

Figure 1.1: Role of NIU



projects. These institutions would work in the spirit of partnership with Government, helping to overcome some of the challenges of a pure MSP/vendor model. They would participate in high-level design, specification of requirements, proof-of-concept studies, while strategic control is retained within Government. For actual implementation, the NIU then contracts with vendors from the market for specialised services while being completely responsible to the Government for committed deliverables and service levels. The proposed structure is depicted in Figure 1.1. It is believed that the NIU model would substantially overcome the problems faced by the Government in implementing the projects with in-house skills or through the MSP/vendor model.

Projects that can benefit from an NIU structure may have one or more of the following characteristics:

1. Projects that span multiple levels of Governments — Central, State, Local (Chapter 5)
2. Projects that span multiple Government departments
3. Projects that span multiple stakeholders, where the network externalities of a thriving ecosystem around the Government developed platform is essential for success
4. Projects that require significant business process re-engineering to leverage technology
5. Projects that aid a sovereign function of Government

1.2. National Information Utilities (NIU)

As conceived by the Group, NIUs would be *private companies with a public purpose*: profit-making, but not profit maximizing. This concept is not a new one; some comparable examples are NSDL (Box 1.1), NPCI (Box 1.2), and CRIS (Box 1.3).

An NIU would make available essential infrastructure for public service. Such institutions can make it possible for Government functions to be carried out efficiently, allow feasible projects to be designed, and thus foster economic development. Well functioning NIUs have a net positive effect on society, like other infrastructure institutions.[1]

For projects in Government, at a high level, the two major tasks are *policy making* and *implementation*. The policy related tasks such as policy formulation and policy

[1]Market Infrastructure Institutions (MIIs) described in the Report of the Committee (chaired by Bimal Jalan) are a closely related concept: http://www.sebi.gov.in/commreport/ownershipreport.pdf

Box 1.1: National Securities Depository Limited (NSDL)

1. NSDL is a company incorporated under the Companies Act, 1956, and regulated by SEBI.
2. The principal sponsors UTI, IDBI, and NSE are required to hold a minimum of 51% stake. Principal sponsors give an undertaking that they stand responsible for all operations carried out by NSDL.
3. Other stakeholders include SBI, banks, and depository participants.
4. Paid-up equity of Rs.80 crores; Net worth above Rs.100 crores, as required by SEBI regulations.
5. There are no Stated restrictions on listing NSDL in the stock exchange, other than the 5% maximum stake requirement for any shareholder; but only depository participants can be shareholders.
6. NSDL is managed by a Board of Directors; it is governed by its bye-laws, and its business operations are regulated by business rules.
7. Though NSDL is a profit-making company, it does not have quarterly targets and does not work towards maximizing profits. Windfall profits and increase in revenue volumes are adjusted through reduction in tariffs and charges.
8. Operating model involves:
   (a) Outsourcing to external vendors/ service providers. Certain activities like system administration, DB administration, UAT, regression and volume testing, requirements gathering, system analysis are done by in-house functional analysts and engineers
   (b) Operating expenditure based contracts with Government customers
   (c) Capital expenditure based / fixed price/ time-material contracts with vendors/ suppliers
   (d) NSDL has the autonomy to pay market-linked salaries to its employees. The compensation levels are benchmarked with financial services sector and IT sector.
   (e) NSDL is not bound by Government procurement regulations

enforcement should be carried out by Government. The NIU would be primarily responsible for technology-related aspects of implementation, bound by tight service level agreements (SLA), and subject to periodic audits. The project must be designed so that strategic control is retained within Government.

1.3. Institutional framework and strategic control

1.3.1. *Independent management*

The structure of the NIU should be such that it should be able to work without the need for day-to-day guidance and advisory from the shareholders/members/Board. The management should be independent and empowered to take quick and efficient business decisions pertaining to attracting and retaining talent, procurement, rapid response to business exigencies, adopting new technologies etc. The independence of the management is linked to the financial independence of the NIU. Therefore, the NIU should be able to get funding independently and have a self-sustaining financial model (for e.g. levy user charges/ charge for services or a combination). The entity should be empowered to commit and sign appropriate SLAs with customers and vendors.

1.3.2. *Strategic control within Government*

Given the sensitivity of the role that the NIU will play, it is necessary that strategic control be retained within Government. Strategic control primarily should be focussed

Box 1.2: National Payments Corporation of India (NPCI)

1. Incorporated as Section 25 company under Companies Act, 1956
2. Ten promoter banks (State Bank of India, Punjab National Bank, Canara Bank, Bank of Baroda, Union bank of India, Bank of India, ICICI Bank, HDFC Bank, Citibank, and HSBC).
3. Authorized capital is Rs.300 crore; paid up capital is Rs.30 crores. Equity contribution in NPCI is not considered as an exposure to financial markets.
4. Board composition: Chairman, nominee from RBI, nominees from promoter banks, MD and CEO.
5. Intent was to involve the top banking community as shareholders to the company.
6. The core business of NPCI is *inter-bank transaction processing*
7. NPCI termed as Deemed public sector; it falls within the ambit of CVC and RTI due to its public sector status.
8. Challenges faced by NPCI include:
   (a) Pricing pressure from competition
   (b) Service management expectations
   (c) Restrictions on scaling the organization due to Section 25 status
   (d) Having customers as board members

on the vision and outcomes of the project, rather than controlling the functioning and management of the day to day affairs of the NIU. Providing flexibility to the NIU is not necessarily against achieving the broad objectives and outcomes of the project.

Strategic control can be achieved by having a strong dedicated team within Government *inter alia* to drive policies, design a suitable solution architecture, supervise execution, frame appropriate contracts, adopt outcome based pricing, evolve SLAs, and conduct independent audits.

1.3.3. *A flexible institutional framework*

In order to evolve an operational model that would help in achieving the twin objectives of independent management within the NIU, and retention of strategic control within Government, the Group evaluated two alternatives; namely a Society (registered under *The Societies Registration Act, 1860*) and a Company (registered under *Companies Act, 1956*).

A Society is governed by its bylaws, which are specifically defined for each Society. The Societies Registration Act, 1860, provides full flexibility to the members of the Society to define the bylaws based on which the society is to be governed and managed. A Company is governed by Companies Act, 1956. Under the Act, there is a clear distinction between Management and the Governing Body (Board of Directors). The Act also lays down the roles and responsibilities of Directors, including the Managing Director.

A society can be created with bylaws that allow for independence of the management team with regard to operations, including HR policies and compensation norms, procurement process, and financial decisions. However, in order to retain strategic control, the society needs to be controlled by Government and its processes may have to be aligned with Government processes.

Box 1.3: Centre for Railway Information Systems (CRIS)

1. CRIS has been formed as a society governed by its own bye-laws. It was registered as a society under the Societies Registration Act, 1986.
2. CRIS's interface with the Ministry of Railways is managed through a Directorate at the Ministry. It is headed by a dedicated Managing Director.
3. The society's structure requires it to approach the Ministry of Railways for financial approval.
4. CRIS has avenues to raise resources through levy of 10% service charge with respect to the procurement of goods and services it undertakes with respect to various projects. However, in recent times, even this service charge is being reduced / eliminated due to cost cutting by the Ministry.
5. Challenges faced by CRIS include:
   (a) Constraints on financing of projects
   (b) Limited business continuity due to staffing by officers on deputation for short periods
   (c) Interfacing with the Ministry through the Directorate can sometimes be sub-optimal and slow

On the other hand, a company's management is provided with the requisite empowerment to operate independently with regard to day to day operations and yet be accountable to the Board. The Companies Act, 1956, provides for more elaborate and rigid norms (as compared to a society) with respect to accountability and transparency. The governance structure of a Company allows for Government to retain strategic control (by virtue of being a shareholder and also a customer), without impeding the independence of its management.

In the context of executing complex projects in Government, a company structure is preferable over a society due to greater ability to raise funds and it allows for financial independence, operational flexibility, quicker decision making, greater accountability, and transparency. In the context of a society, the ability to attract different kinds of capital is limited and the structure is not viable for the public-private nature as envisioned in the long term.

The Group therefore recommends that the NIU should be structured as a company with limited liability and be subject to sound corporate governance norms, such as those required for listed companies. While the company should not be listed on a stock exchange, the board composition, accountability, and transparency norms for NIUs should be the same as prescribed for listed companies.

1.4. Ownership

The following characteristics would be appropriate for NIUs:

1. Total private ownership within NIUs should be at least 51%. As a paying customer, the Government would be free to take its business to another NIU, if necessary. At the same time, the Government could moderate the functioning of the NIU by virtue of being the owner, through its position on the Board.
2. The ownership share of the Government in an NIU should be at least 26%.
3. No single private entity should own more than 25% of the shares in an NIU. Institutions that have a direct conflict of interest (eg. IT companies) should not be permitted to be shareholders.

4. An NIU should not go for an initial public offering or list itself on public exchanges.
5. NIUs should be dispersed-shareholding corporations with a professional management team who are not owners.
6. A re-mutualisation approach may be thought of, wherein the shareholders of an NIU are the entities who stand to greatly benefit indirectly from its success. This would help align their incentives to the impact of the NIU upon society, as opposed to a focus on dividends and valuation.
7. An NIU should preferably have a net worth of Rs.300 crore. This will ensure that the NIU is well-capitalized, can hire the best people at competitive salaries, and invest adequately in infrastructure, so that it can manage large-scale national projects.
8. The articles of association of the NIU may include a cap on dividend payouts, to ensure that the incentives of the owners do not drive it towards profit-maximization.

1.4.1. *Desirable features*

NIUs are important institutions, since they aid the functioning of Government. Due to various factors such as a large upfront sunk-cost, economies of scale, and network externalities from a surrounding ecosystem, they are essentially set up as *natural monopolies*. It is thus essential that a monopolistic operator is obliged to provide access to a competing NIU, when one emerges. For example, the Depositories Act, 1996, requires full interoperability among all depositories. NSDL was initially set up as the first depository, whose creation was facilitated by Government. However, when CDSL emerged, the customers benefited from interoperability across depositories.

The following are desirable features for effective functioning of an NIU:

1. **Self-financing:** The NIU should be capable of self-financing its operations and providing for its sustenance in the near future.
2. **Make reasonable profits:** The NIU should endeavor to generate reasonable profits in order to be self-sustaining. The NIU should levy reasonable charges on its users without abusing its dominant position. The NIU must not maximise profit or valuation. Salaries of employees should not be linked to profits. The salaries should be competitive and market driven, to ensure that the best quality of people for the job can be hired.
3. **Net worth:** The net worth of the NIU should be available as a last resort to meet exigencies and ensure that it is able to remain as a going concern.
4. **Professional standards and competitive practices:** The NIU must maintain the same professional standards in all its dealings including dealings with its competitors, its technology providers and related entities. It must be able to maintain its integrity by being unbiased while dealing with all such entities.
5. **Transparency:** The NIU should maintain utmost transparency in its operations. The NIU on its website should at least make disclosures that are mandated for a listed company.
6. **Technology:** The NIU should be willing to invest in technology for increasing efficiency, reach and economies of scale.
7. **Competition:** NIUs would have characteristics similar to those of monopolies. Hence, it is essential to create enabling conditions that allow new entrants to enter the market, with necessary safeguards in place.

1.5. Allocation of tasks and responsibilities

The Government-NIU relationship must be in the spirit of a partnership, rather than that of a vendor and customer. The relationship may be defined by an Agreement, which contains the allocation of tasks and responsibilities between the Government and the NIU, financials, and SLAs.

In the early phases of a project, during incubation, the Government may also have to be actively involved with implementation of technology. The NIU should also engage the services of domain experts from within and outside the Government during incubation and subsequent stages of implementation. Both, the Government and the NIU should have teams that are dedicated to the project, which will facilitate smooth decision making.

The concerned Department that owns the project and is responsible for its successful implementation should lay down clearly the project goals and charter. Business change is the driving force, and technology is an enabler. Therefore, a Mission Strategy Document for the project that *inter alia* details the functions, and capabilities of the IT system, which would assist in bringing about the desired business change, should be prepared.

The Department should recognize the capabilities and limitations of the technology solution, while the NIU should perceive its responsibility as extending beyond merely meeting a technical or legal requirement under the Agreement, but as providing a holistic service to achieve the projected business change.

2

Human resource policies

2.1. Background

All projects that aim at effecting a business change through enhanced use of IT systems, are first of all, governance projects. The success of a complex project with multiple objectives and multiple stakeholders requires a strong Mission Execution Team that is capable of driving all business and technology issues.

This team should get the total support and involvement of the top management within Government, acceptance of change and use of IT systems by all, particularly, the host of end users. Investment in *peopleware* and effective harnessing of human capital deployed for conceiving, designing, implementing, maintaining, and running of such systems is indeed a clear need in the context of large projects such as those under study by this Group.

These projects require a diverse mix of skills, ranging from domain specific knowledge on business issues and managing large decentralized organizations, to specialised skills in domains such as technology design, vendor development and informed buying, contract facilitation and monitoring, law, relationship building, communication and outreach. Today, Departments have officers who are business specialists, with a deep understanding of the Department's business and domain knowledge as well as officers who are generalists, who manage the running of a large decentralized organization. For the execution of large complex projects that include mission-critical IT systems, it is important to complement the skills within Government with specialised skills from the private sector.

The Group had the benefit of interaction with officers of Departments that have implemented large projects with a significant IT component and based on the same, the following human resource challenges within Government have been identified as requiring consideration:

1. Absence of leadership and active ownership of projects
2. Outdated recruitment processes and methodology
3. Inability to pay market salaries for specialised skills
4. Lack of diverse opportunities and variety in assignments
5. Lack of avenues of continued enhancement of professional skills and career growth opportunities

6. Non-conducive work environment
7. Outdated performance evaluation and preference for seniority over merit
8. Untimely transfers of officers posted to handle certain project functions

2.2. Key recommendations

2.2.1. *Leadership and active ownership*

The Group is of the view that strong support from the top management within Government, leadership at the level of project implementation, and ownership and commitment at various operational levels are necessary concomitants of success of any project. The concerned Department should put in place a high level body that will review the progress of the project during its implementation and later evaluate the realization of benefits and objectives on a periodic basis.

Further, every project should have:

1. A dedicated **Mission Leader** within the Government Department responsible for the project
2. A dedicated **Mission Execution Team** should support the Mission Leader
3. The Mission Leader should have the freedom to choose the Mission Execution Team from within or outside the Government

2.3. Recommendations for the Government team

2.3.1. *A dedicated Mission Leader in Government*

Typically, complex mission-critical projects in Government are anchored under an officer of the level or seniority of a Joint Secretary. Often, this Joint Secretary has a number of other responsibilities also that they may have to attend to on a daily basis. While this model works well for projects that are already on course and only day-to-day operations have to be managed, it does not work well for new and complex projects that are getting off the ground.

Every mission-critical project in Government should therefore have a dedicated Mission Leader who holds the rank of a Joint Secretary or Additional secretary or above in the Government of India. If the project is being implemented within a Department, the Mission Leader should directly report to the Secretary. The Mission Leader should be fully responsible and empowered for all aspects of the project: policy, decision-making, human resources, finance, procurement, and all other aspects of implementation. The Mission Leader must have skills and expertise (including experience with IT projects) specific to the project, which must be corroborated by a quantifiable track record. The selection of the Mission Leader should be open to all officers within Government, and through open advertisement.

2.3.2. *A dedicated Mission Execution Team in Government*

The Mission Execution Team is a dedicated team that is focussed on project implementation. A diverse set of skills are required for successful execution of complex projects. These skills include intimate familiarity with the Government processes, specialisation in verticals such as technology, outreach, law, as well as the ability to manage a large decentralized organization, among others. The Mission Leader should have full flexibility in hiring the Mission Execution Team, combining people from the public and private sectors. This team, including the Mission Leader, should have adequate tenure (at least 5 years) for purposes of continuity, so that institutional memory can be created and retained.

2.3.3. *Recruitment and tenure of the Mission Execution Team*

Professionals may be hired from within the Government, or from the private sector into the Mission Execution Team in a number of ways as indicated below:

1. Posting suitable officers to the project from the same cadre;
2. Inducting officers on deputation from other departments at suitable compensation under the Central Staffing Scheme; persons selected through this process should be given a tenure co-terminus with the project timelines, and be given all benefits of promotion while working on the project, so that they will not suffer on account of non-reversion to their cadre at the time of promotion; and
3. Infusion of talent from the private sector by way of lateral entry.

Other modes of staffing the Mission Execution Team that could be considered are as follows:

1. Hiring professional resources on contract basis;
2. Appointing consultants at market rates on contractual basis;
3. Recruiting sabbaticals from industry, who continue to be employed by the parent organization, but spend all their time on the Government project;
4. Recruiting volunteers who come from various walks of life through a well-defined volunteer selection process; and
5. Recruiting students from various colleges and universities as interns through a well-defined internship program

Given that a diverse mix of people may be inducted into a project, it is essential that all recruits should be made familiar with Government rules and procedures, perhaps through a short training course. With the exception of recruiting volunteers and sabbaticals[1], the rest of the methods of recruitment are provided for even now. The recommendations of the Sixth Pay Commission on contractual appointments[2] may be referred to in this context. These provisions should be more widely used for the five projects in view, and also other projects that may be launched in the future.

2.4. Staffing of the NIU team

An NIU, on the other hand, can hire professionals from the market at market salaries. Just as the Government team will have business specialists, and experts from other domains, so should the NIU have a management team with the right domain knowledge, and other essential expertise in areas such as technology, law, and outreach. The NIU should also take on its staff, professionals from the Department, who have the requisite business domain knowledge, so that the IT systems they develop and implement is backed by people with relevant domain experience.

2.5. Database of IT Projects and Centres of Expertise

The Group is of the view that the Government should set up a Database of all IT projects implemented in the public sector, including the PSUs. This database should contain comprehensive details of the individual projects and the key personnel associated with the project. Such a database will assist in identifying the IT talent available in the country, which can be tapped to meet the specific or general requirements of any

[1] Hiring sabbaticals, volunteers, and interns at UIDAI: http://uidai.gov.in/index.php?option=com_content&view=article&id=154&Itemid=15

[2] Sixth Pay Commission (Paragraph 1.2.6): http://india.gov.in/govt/paycommission.php

similar project of national importance. Further, the task of drawing IT professionals on deputation from different departments and PSUs as also on contract basis from the private sector would be facilitated. Secondly, *Centres of Expertise* within the country would need to be identified for providing assistance by way of project consultancy through accredited professionals and advanced training in the field of IT management.

2.6. Capacity Building and retention of in-house staff

The Group suggests the following measures for capacity building in the departments embarking on large, complex projects with mission-critical IT systems:

1. The training curriculum for the existing workforce of various services should include training on the technical aspects of IT systems, project management and evaluation, procurement management, governance issues, and change management.
2. Mid-career programs should also be designed in such a way that senior officers are not only able to provide the required leadership but also coach and mentor junior managers.
3. All induction programs and furbisher programs for employees should include basic knowledge of IT systems, hands-on training in departmental IT projects and effective use of information flowing from Computer applications.
4. In-service personnel, who already possess technical knowledge should be trained in the latest technologies and in fields in which they like to specialize.

As regards retention of in-house staff on IT projects the following measures are suggested:

1. In-service officers deployed in IT functions should be provided with *IT professional allowance* on the lines of the training allowance at the rate of 30% of their remuneration. Such a provision is justified for the following reasons:

   (a) In-service officers deployed in IT functions are entrusted with the important task of preparation of operation manuals and conducting of training programs for end users and the ICT aware staff on a continuing basis.

   (b) These professionals are expected to possess specialised skills in evaluation, procurement, and management of technologies, and maintain communications with various stakeholders. The IT skills of these teams require regular refresh to enable them to engage meaningfully with IT vendors, optimize investment in IT infrastructure, and ensure that systems development remains aligned with business requirement.

   (c) Such officers are part of the Mission Execution Team and have to put in long hours of work.

   (d) Strong IT and domain skills in Government teams ensure that strategic control remains within the Government.

2. The Performance Linked Increment Scheme as suggested by the Sixth Pay Commission for Central Government employees, should be implemented supplementing the same with performance linked training programs in special skills.
3. A scheme of non-monetary incentives such as public acknowledgement of their contributions, certificates of outstanding performance etc. should be instituted with a view to motivating both in-service officers and contracted personnel.

4. Full opportunity should be provided for every individual to equip himself for higher levels of responsibility through individual and group assignment and training programs to ensure that his/her needs are satisfied. In order to enable employees to develop multiple IT skills, both technical and managerial, they should be provided with work diversity in different application areas and different technology. This would enlarge the opportunity spectrum available to the employees.

2.7. Conducive work environment

Other measures suggested for consideration for creating a conducive work environment are as follows:

1. The in-house end users of information systems, who are at the front end, are generally the least prepared to handle the change that is sought to be effected by extensive automation and e-governance techniques. Without user participation in planning the overall strategy of implementation and in-systems development and testing, it is difficult to buy their support and ownership of the system. End users should be able to assist in on line processing of work, get information from the system and also provide inputs for improvement. Such end users should be provided appropriate training and support and encouraged to make their own contribution to the success and continuous improvement of the project outcomes.
2. With a view to raising the motivation levels of in-house employees, creation of a proper work environment is a clear necessity. Towards this end, team formations should be done with care and thought so that those who are in the initial phase of their careers are placed along with supportive co-workers, who are willing to coach and mentor them. Managers should also be trained in coaching. Employees should be sensitized about the vision and values of the organization and encouraged to contribute towards realizing the same. Access to learning by choice in areas of interest to the employees and also useful to the organization and availability of feedback from managers in order to measure their contributions and gain greater control over their work should be part of creation of the right work environment.

2.8. Performance Appraisal

The discussions held by the Group have revealed that the present appraisal system within Government has several salutary aspects, such as filing of a resume by the employee and review by the higher authority. There are detailed instructions explaining the way the appraisal should be conducted. Yet, there is a widespread perception that the system is beset with shortcomings.

The Group is of the view that the method of performance appraisal has to be reconsidered, by redefining the purpose and principles, conducting a job analysis, obtaining employee feedback, reviewing standards of objectivity, conducting training for both managers and employees and reviewing/evaluating the results of the system. Greater objectivity and according appropriate weight to the overall contribution of the individual has to be given due consideration. Since increasingly, Government is undertaking tasks which demand greater professional skills, such as IT skills, merit should be given primacy over seniority within a given band of eligible appointees. Adoption of performance management techniques would be particularly relevant for appraising the performance of in-service officers entrusted with the task of implementation of mission-critical projects.

3

Contracting

3.1. Background

Many an IT project fails due to shortcomings in contracting. The contracting process defines the placement of tasks; which tasks are kept within Government, and which are outsourced. As discussed in Chapter 1, a contract for large complex project is likely to suffer from over-specification or under-specification, especially if there exists no precedent or proof-of-concept study. This chapter provides general recommendations for good contracting

A study on *E-Governance & IT Services Procurement: Issues, Challenges, and Recommendations*[1] has been published by NASSCOM. This includes a review of Government procurement guidelines, and highlights challenges from the Government's perspective as well as the industry perspective.

Contracting is a well-understood subject within Government. Nevertheless, the following general aspects that impinge on the relationship between the supplier and the Government merit a mention as they have equal relevance for a relationship in the nature of partnership or vendor customer model.

1. The solutions proposed by the supplier should focus on and meet the business needs spelt out by the Department owning the project and not just the technical/operational requirements.
2. Through the lifecycle of the project the supplier should produce realistic plans, including timeframes, resources, technology, mode of delivery and financials, and align the same with the business needs.
3. The supplier should as far as possible ensure continuity in employing trained personnel on the project from start to the steady State.
4. Both should share in a timely manner all information about technical/financial/personnel problems.
5. Both should set up a mechanism for co-operation and dialogue.
6. Both should agree and document change control processes,address risk factors and avoid informal and cosmetic changes.

[1] E-Governance & IT Services Procurement: Issues, Challenges, and Recommendations (NASSCOM): http://egovreach.in/index.php/pages/national

7. Both should recognize that estimates of price, timeframes should be realistic and achievable.

3.2. Contracting with National Information Utilities

The success and timely completion of a project depends a great deal on the completeness of the contract. The ideal contract defines all requirements exactly, and addresses all possible contingencies — it is a risk management tool. Based on this ideal contract, the ideal firm can bid perfectly, and execute the contract as specified.

However, it is not always possible to achieve the ideal of specifying all requirements/contingencies with respect to complex IT projects right at the time of inception. Both over-specification or under-specification should be avoided.

As described in Chapter 1, NIUs work in the spirit of partnership with Government. The NIU is an intermediary of sorts, between the Government, and the IT vendors that build the project. An NIU-based approach is an incremental approach. An NIU approach also leads to a clean separation of roles in the steady State, where the Government focuses on policy, and the NIU focuses on implementation and execution.

The Government-NIU relationship can be defined through an Agreement. The Agreement outlines the broad project goals, placement of tasks, financials, SLAs, and most importantly, embodies the spirit of partnership. The Agreement should include the following:

1. Scope of work
2. Activities to be undertaken by NIU
3. Obligations of the Government and NIU
4. Financial Arrangement
5. Service Level Agreement
6. Business continuity plan upon exit

This relationship is further defined through ownership and governance structures for NIUs, which are set up as private companies with a public purpose. Even though the NIU is set up as a natural monopoly, the ownership and governance structures combined with the fact that it is set up to service just one customer at a pre-defined service level, act as the right checks and balances.

An example of the risk management methodologies adopted in the TIN Agreement is provided in Box 3.1.

3.3. Aspects to be covered in the agreement with NIU

The Agreement between the Government and the NIU should cover in clear terms all the aspects discussed in the succeeding paragraphs in this section.

3.3.1. *Scope of work*

The scope of work is a high-level functional (but complete) description of the project at hand. It clearly defines the tasks to be undertaken by the NIU, and defines the milestones and deliverables. Further details may be provided in other detailed specifications documents.

Box 3.1: Risk management in TIN

Income Tax Department (ITD) provided for adequate measures to ensure the quality of service in TIN. These measures included:

1. An Agreement signed with NSDL that covered:
   (a) Scope of services by NSDL
   (b) Responsibilities of NSDL and ITD
   (c) Regular MIS to ITD
   (d) ISO 9001-2000 certification for TIN processes
   (e) ISO 27001 certification for NSDL Information Systems security practices
   (f) Periodic Review of TIN operations jointly by ITD and NSDL
   (g) Third party audit to monitor quality and security of the systems and processes established by NSDL
2. Service Level Agreement signed with NSDL to ensure that NSDL continues to provide services as required by the department.

3.3.2. *Activities to be undertaken by NIU*

In order to accomplish the tasks assigned to it, the NIU may be required to set up infrastructure and implement supporting processes. These activities should be defined at a functional level to the extent possible under this head.

3.3.3. *Obligations*

The obligations of both, the Government and the NIU should be articulated as clearly as possible in the Agreement. These obligations are necessary conditions for the success of the project, and will be monitored through SLAs.

3.3.4. *Financial arrangement*

Typically fixed-cost pricing is preferred for systems that have reached their steady State. However, the Agreement between the Government and the NIU is at a functional level, unlike traditional tendering, which is often at an implementation level. As a result, it is essential that outcome-oriented pricing be adopted. The pricing should be for the accomplishment of the business objectives on a per transaction basis. The onus is then on the NIU to figure out sizing, scaling, storage, capacity etc.

3.3.5. *Service Level Agreement*

Very strict and detailed SLAs are essential when Government contracts out a project to an NIU on the basis of an Agreement. It is only through SLAs that the obligations can be monitored, and the financial arrangement implemented. The agreement should allow for strict penalties if SLAs are violated. The Government should also appoint Independent auditors to ensure that the NIU continues to provide services as agreed upon.

3.3.6. *Business continuity plan upon exit*

In the event that the Government wishes to terminate the relationship with the NIU, there should be a business continuity plan outlined in the agreement. There should be

an elaborate continuity plan as per industry best practices to ensure that the project process does not get halted during exit of the vendor or during transition. For this purpose, the contract should lay down a clear handover/transition plan, the required logistics for transfer of hardware/software, migration of data, provision of a transition team, data security and confidentiality, among other things.

4

From startup to going concern

4.1. Background

The startup phase of a project may be defined as the phase from incubation to the point where a long-term institutional capacity is set up to manage operations on a regular basis. The challenges faced by a project during the incubation phase are very different than challenges faced in steady-state operations. The Government may have to play an active role during incubation, shifting to a largely regulatory role in steady-state.

Effective incubation can help the project rapidly get off the ground. The incubation phase includes issues that range from mundane issues such as setting up an office and hiring staff to devising incentive compatible solutions that are agreeable to all stakeholders.

This chapter presents a broad framework for incubation that can help projects get off the ground rapidly. An example of incubation recommendations made in the context of the NTMA is presented in Box 4.1.

4.2. Institutional framework for the project

One of the first steps in the incubation of a project is the creation of a suitable institutional framework. Depending on the nature of the project, it may either be housed within a Department, or in a new institution created with the specific purpose of executing the project. Various institutional frameworks that were examined in the context of NTMA are described in Box 4.2.

4.3. Incubation of a new National Information Utility

While a project itself may be housed within one of various available institutional frameworks, an NIU that serves the project should necessarily follow the structure as described in Chapter 1.

In the case that a new NIU is being created to support a particular project, it can be incubated within an existing NIU. Subsequently, when the project achieves some level of maturity, the project team and project assets (tangible and intangible) can be spun off

Box 4.1: Incubation of National Treasury Management Agency

A committee headed by Dr. Jehangir Aziz has proposed **Establishing a National Treasury Management Agency (NTMA)** The report has been shared with regulators, State Governments and other relevant agencies for their comments. The report is essentially a Mission Strategy Document that discusses the need for the NTMA, the legal framework, stakeholders, and the process of incubation. It also includes a draft of the National Treasury Management Agency Bill. Chapter 8 of the report outlines the following steps for incubation:

1. The NTMA would commence operation as a non-statutory office of the Ministry of Finance, as was done in the early days of SEBI, IRDA and PFRDA. A mechanism will need to be arranged for MOF to give the NTMA a budget in this phase. The key tasks that need to be put into place at the outset are:
   (a) Office premises
   (b) Setting up an organisation chart
   (c) Establishing an HR process; recruiting key individuals into this organisation chart
   (d) Establishing the advisory board
   (e) Setting up a series of outsourcing relationships
2. Establish databases about the Central Government's debt and contingent liabilities, along with a website
3. Establish a research and analytical capability
4. Plan out bond market processes and market mechanisms for bond issuance and trading
5. Stakeholder analysis and reaching out to market participants
6. Linkage of the NTMA IT platform with IT platforms of Government, exchanges, depositories, and investors
7. After the NTMA is set up, the core debt management functions can be transferred from RBI to the NTMA.

into the new NIU. The original NIU, in this case, should be compensated appropriately for the resources it deploys.

4.4. Mission Strategy Document

At the outset, the project should publish a Mission Strategy Document that describes the project, the stakeholders, the broad legal framework, the solution architecture, the nature of the platform and role of the ecosystem, and potential pricing. The strategy may evolve over time, but the guiding principles should be sound and remain unchanged. The process of creating such a document also helps set and manage the expectations of stakeholders, and ensures that the solution is designed in a way that is acceptable to all stakeholders.

The report of the Working Group on *Establishing a National Treasury Management Agency*[1] can serve as the Mission Strategy Document for the NTMA. The UIDAI published early on, the *UIDAI Strategy Overview*[2] that described the strategic vision, from which many aspects of implementation have been derived.

[1]Establishing a National Treasury Management Agency: http://finmin.nic.in/reports/Report_Internal_Working_Group_on_Debt_Management.pdf

[2]The UIDAI Strategy Overview: http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf

Box 4.2: Institutional frameworks considered for NTMA

In the report on **Establishing a National Treasury Management Agency (NTMA)**, the Working Group (WG) considered various institutional frameworks:

1. **An Executive Agency:** The WG recommends an Executive Agency as a sound interim step, but suggests that such a structure would face resource constraints, and risk being perceived as closer to the Centre rather than a neutral agent of Central and State Governments.
2. **A Company:** While providing flexibility and independence, the WG noted that regulatory certainty and predictability are crucial when an agency implements the Government's decisions on a core sovereign function such as debt management, and that judicial decisions on company law may affect this regulatory certainty.
3. **A Society or Trust:** These structures were rejected as impractical as they would limit the range of financial instruments that NTMA could deploy.
4. **A Statutory Body:** The WG recommended that the NTMA be a Statutory Body for the purposes of operational flexibility, accountability to Central and State Governments and to Parliament, financial expertise, and for the ability to prioritise public policy objectives rather than tactical trading objectives.

4.5. The right team

It is essential that the best teams be put in place within Government and within the NIU. This should be the first and foremost priority of all projects. The chapter on human resource issues (Chapter 2) describes general principles for putting a project team in place within Government and in the NIU.

4.6. Consultations with stakeholders

Consultations with stakeholders early on in a project is crucial to set it along the right trajectory. At a minimum, stakeholders include:

1. Multiple levels of Government, or other Government Departments
2. NIU
3. Banking system (if funds are involved)
4. Service providers whose services are essential for the project
5. Customers and end-users

Depending on the nature of the project, it may be necessary to hold consultations with various other Departments, trade associations, marginalized groups, etc. These consultations are necessary to ensure that an incentive compatible solution is designed, which is acceptable to all stakeholders.

4.7. Legal framework

A legal framework, with enabling policies may be necessary for a project to go live. This may require passing a Bill, modifying subordinate regulation in Central and State Acts, or in some cases, a constitutional amendment. A strong legal team working with all stakeholders is a must for every project.

4.8. Incremental rollout

The project should be rolled out as soon as possible, and iterated rapidly, rather than waiting to roll out a perfect system. This represents a recent shift in the way large IT projects are implemented today; the style having been popularized by modern internet firms processing millions of transactions daily. Such a rapid iterative rollout process makes it possible to get customer feedback early on, and allowing mid-course corrections as necessary. It also helps keep the project teams motivated and excited.

4.9. Government-NIU relationship during incubation

1. The Government should have a dedicated Mission Execution Team as described in Chapter 2. The Government's role is to set policy, co-ordinate with other departments, and provide strategic direction, whereas the NIU focuses on execution and implementation.
2. In the early stage, the Government agency / Department works alongside the NIU in an entrepreneurial spirit of trying to understand the challenges and design a system that will deliver results. Many research and development sub-projects and proof-of-concept studies may get initiated at this stage. The Government and NIU jointly define the requirements post these learnings.
3. As the system starts falling into place, the role of Government changes to:
   (a) Conducting proof-of-concept studies
   (b) Giving feedback on misfeatures, bugs and additional specifications
   (c) Setting up the institutional capability for scaling
4. Once the rollout is completed, the Government's role shifts largely to that of a customer. It should compute metrics of performance of the system in all respects such as performance, cost, accuracy, and release these into the public domain. Quarterly reviews of the performance of the system should be undertaken at the highest levels. A variety of external experts should be brought in on a regular basis to study the functioning of the system, and to critique it along with proposals for improvement.
5. Even after these complex IT systems are fully running, none of these systems ever stand still. The very success of a project generates an array of areas where extensions are possible, and the magnitude of scale-up that can arise out of success can be quite dramatic given the size of India. A consultative process needs to be established for agreeing on new features of the system and ongoing change management.

5

Multiple levels of Government

5.1. Background

A class of national infrastructure projects have been implemented successfully today, which include a stock exchange (NSE), depository and Tax Information Network (NSDL) etc. This class of applications has typically had a single owner and could be Centrally implemented. A new class of applications such as GST, NPS, and EIN will span multiple levels of Government where Central, State, and Local Governments will all have jurisdiction and some role to play in successful implementations. This chapter deals with the concerns in the implementation of IT projects within a federal structure with multiple stakeholders, and recommendations to address those concerns.

5.2. Decentralized governance

Decentralisation of Government is a healthy feature of democracies when it produces a tighter link between accountability through elections and the delivery of local public goods. States have constitutional autonomy in certain areas under the Indian constitution. IT systems designed as a single application may be perceived to shift the balance of power within the federal structure.

Every Government at every level that is touched by an IT project is a stakeholder. Thus, a project such as GST that requires buy-in from all States, or EIN, which spans all levels of Government, is unlikely to succeed, if the IT systems are designed and operated by one of the Governments. There is always the fear that a non-transparent system, with control concentrated with some of the stakeholders may affect the autonomy of the others. This may happen in subtle ways due to inefficiencies, delays, and errors, which are not uncommon in complex IT systems in early stages. A critical aspect of the success of such IT projects is that the solution must be incentive compatible for all stakeholders. Common functions should be included in a single application shared by all stakeholders.

IT projects that span multiple levels of Governments may be classified into two types:

1. Projects such as GST, NTMA, and EIN where the NIU aids the core function, or aids carrying out a sovereign function of multiple levels of Government.

Box 5.1: Solution design for GST

The Common GST Portal has been designed as follows:

1. Common minimum functionality (PAN registration, standardized return filing, and standardized challans for payments) is built into the Common GST Portal
2. Only information flows through the Common GST Portal, whereas funds flow through the banking system
3. Given that GST will be an important source of revenue, the funds arrive in almost real-time from the taxpayer, through the banking system, into the State and Central Government treasuries. Thus, the constitutional autonomy of all Governments is respected by the IT system design.
4. The Common GST Portal passes the information on returns and challans immediately to the tax administration systems, while enhancing this information with intelligence gathered from matching returns
5. The design and implementation of the Common GST Portal has started while policies such as tax rates are being debated and the legal framework is being put in place

2. Projects such as NPS, where the core function is carried out by a Central agency, but co-operation among Government agencies is required for the purposes of uniformity, standardization, interoperability to maintain levels of service and drive economies of scale.

5.3. Need for a single application

IT systems naturally lend themselves to development as a single application developed by one team. A single application may be deployed in a decentralized environment, but its development must necessarily be centralized.

IT systems developed as a single application encourage standardization, drive economies of scale, higher efficiency and increased productivity. Systems thus developed are efficient in the use of public funds, which otherwise may be spent on multiple platforms implementing similar but incompatible technologies multiple times. Such systems can be developed so that they can be customized at every deployment point, but it still operate as a unified application. This also offers a uniform customer experience for all interactions with Government.

As communication networks become more pervasive, technology solutions are getting increasingly centralized. As an example, rather than storing email on their PCs, people prefer to have their email on the web, and find it convenient to access it anywhere. Banks have moved from distributed branch automation software to Core Banking Solutions (CBS) over the last twenty years. This does not necessarily mean that the software runs in one data centre only. On the contrary, every branch runs an extension of the CBS software itself.

5.4. Solution design for multiple levels of Government

Solutions for projects that involve multiple levels of Government need to be designed carefully. Not only is it necessary to manage stakeholder concerns and incentives, but it is also necessary to ensure that the solution respects the constitutional autonomy of all levels of Government involved in the project. Increasingly, projects that span Central

and State Governments are being undertaken, and going forward, projects that span Central, State, and Local Governments will be undertaken.

Projects spanning multiple levels of Government require consensus building that may take time. Various Governments may also have to create the right legal framework for the project to operate in. The design and implementation of the solution itself takes a long time. These two activities, consensus building and solution design need not necessarily be sequential. The basic design and the nuts and bolts of the implementation can be put in place while policy details are being debated. Eventually, the policies agreed upon are only an input to the solution, and will change from time to time. Work on actually building the IT systems should thus start at the earliest possible date, while policies are reflected within the solution as consensus is achieved.

As mentioned earlier, such projects should also be implemented as a single application while respecting the constitutional autonomy of all Governments involved. Common minimum functionality can be built into a Common Portal, in such a way that its basic functionality can be enhanced by local customizations such as look and feel, local languages, and local policies, to mention a few. Such a design allows for low cost, scale, interoperability, speed, simplicity, a uniform customer experience, and portability of service. The application of these design principles for the Common GST Portal are described in Box 5.1.

5.5. NIU approach to align incentives

The committee recommends the following for projects that span multiple levels of Government:

1. Clearly identify all stakeholders.
2. Form an Empowered Committee of representatives drawn from every stakeholder for all decision making. If this Empowered Committee is large, a smaller Empowered Group may be appointed for carrying out the day-to-day business.
3. Form an NIU for implementation of the IT system.
4. All levels of Government that are participating in the project may become owners of the NIU, so that they have an equal say in the way the NIU conducts its business.

A joint ownership structure as described above helps align incentives across stakeholders and build consensus by giving them an equal say in decision making, and insuring against an uneven distribution of control favouring one stakeholder over another. A common single application also saves costs and dramatically reduces complexity for all stakeholders, while allowing customization and extension as necessary. An example of this strategy in the case of GST is described in Box 5.2.

In the case that all State Governments and Central Government are owners, the Board of the NIU may end up having too many members. The Board may be, in such cases, comprised of about ten members, with equitable representation of Centre and States. The States may also be represented by rotation and by a body that represents all States. Various committees are also necessary to overlook various aspects of the project, and nominees of all States should be co-opted into these committees.

Getting the governance structure of the NIU right calls for a delicate balance. On one hand, Governments by virtue of their shareholding, are owners. On the other hand, the same Governments are customers. For a typical firm, owners and customers are not the same. Thus, if owners are unhappy with the management team, they can terminate the relationship. If customers are unhappy with the service, they take their business elsewhere. However, if one of the owners is also the customer, these checks and balances may not be as effective as otherwise. The recommendations in Chapter 1 on ownership and governance structures of NIUs take these issues into account.

Box 5.2: Goods and Services Tax Network (GSTN)

GSTN is an NIU that is being set up to serve multiple levels of Governments (Central and State) in GST:

1. The Empowered Committee of State Finance Ministers (EC) has appointed an Empowered Group on IT (EG-IT) to oversee the IT implementation at an operational level. The group has created high-level IT plan: **The IT Strategy for GST**, which has been embraced by all stakeholders
2. The IT strategy for GST called out for the need of a Common GST Portal to implement common functionality
3. A team within Ministry of Finance is working on the legal framework necessary for GST
4. A new NIU (GSTN) has been proposed to operationalize GST
5. Upon evaluating current NIUs such as NSDL and NPCI, the Ministry of Finance has decided to incubate GSTN within NSDL
6. It has been proposed by the EG-IT that GSTN be set up as a Section 25 Company
7. The EG-IT has also recommended that Centre and States would have equitable representation on the Board which should comprise of about ten members. The States could be represented by rotation and also by EC (or its successor). In case the funding of the States was routed through EC (or its successor), the Empowered Committee would be considered as the representative of all the States, for all compliance purposes. To ensure participation of a larger number of States in the governance of GSTN, the Board would be supported by additional Committees in which nominees of other States could be co-opted.

5.6. Building a coalition for change

The execution of large complex projects such as GST, EIN, NPS etc. require building a coalition of change. IT, although a major component, is not the only component. Such large scale computerization often involves business process re-engineering. When such sweeping changes are being carried out, inevitably enough, in the larger interests of certainty and uniformity, some of the stakeholders may have to give up some restrictive practices, while some others may have to adopt certain regulation as against their existing regime. Particularly in the context of GST, an additional consideration may be that of encouraging a common market and freer movement of goods and services. With a successful coalition for change, such large and complex projects are more likely to succeed.

Stakeholder analysis is an important step in building such a coalition. Once stakeholder analysis is conducted, incentive-compatible solutions can be built. It is recommended that the project release a Mission Strategy Document that guides the implementation going forward. The process laid out for incubation of Government projects and NIUs in Chapter 4 is designed to foster a coalition of change early on in the life cycle of a project.

Success of large complex projects such as the five unique projects under consideration depends on much more than getting the IT right. Building a coalition for change greatly increases the odds of success, especially in projects involving multiple levels of Government. Some of these approaches are being tried in the implementation of GST (Box 5.2).

Part II

Technology challenges

6

Solution architecture

6.1. Background

The solution architecture of a complex IT project is an important factor for the success of the project. This chapter focuses on retaining strategic control of the project within Government, by working closely with the implementation team on designing the right solution architecture.

The Group deliberated on good software development practices such as project planning, milestones, development frameworks, quality assurance, and user acceptance testing, among others. Given that many of these are implementation level details, which are well understood within industry, and may vary from project to project, the Group is of the opinion that individual projects should make their own choices on software development processes. The Group also does not touch upon common and well defined practices for mission-critical applications such as disaster recovery centres, high availability, 24-by-7 operation, and fault tolerance; these architectural design principles are well understood by software designers and architects. Some of these issues are discussed in the *Guidelines for Strategic Control in Outsourced Projects* released by the Department of Information Technology, Government of India[1].

6.2. Essential elements of a solution architecture

6.2.1. *Map out a long term IT strategy*

At the outset of a project, the IT strategy should be conceived and published as part of the Mission Strategy Document as described in Chapter 4. A functional system diagram should be created that captures the following at a conceptual level:

1. Role of multiple levels of Government
2. Key business processes and workflows (information flow, funds flow, etc.)
3. Integration with various stakeholders

This forms the basis of the solution architecture, and serves as a guide for implementation level details.

[1] Guidelines for Strategic Control in Outsourced Projects: http://www.mit.gov.in/sites/upload_files/dit/files/Guidelines_Strategic_Control_Outsorced_Projects_251110.pdf

Box 6.1: Change management in TIN

The project was subdivided into a number of small components and specific milestones were identified for these components so that the project could be monitored on a regular basis against specific deliverables.

1. **Compulsion to File Returns in Electronic form:** When the new scheme was introduced in FY 02–03, only corporate deductors were required to file returns in electronic form. From FY 04–05, it was made mandatory for the Government deductors to file the returns in electronic form. More segments of deductors were brought in to the mandatory list in due course of time.
2. **Quoting of PAN and TAN in tax payment instrument:** To begin with, taxpayers were allowed to deposit their taxes even without quoting of TAN/ PAN in their challan. Once the system for issuance of TAN and PAN stabilized, ITD made it mandatory for the taxpayers to quote TAN / PAN in the tax payment challan. Today, more than 98% of TDS challan have valid TAN and 95% of non-TDS challan have valid PAN.
3. **Preparation of e-Returns:** A simple ASCII text-based file format for submission of e-Returns was published. Any software designer or platform provider could prepare returns in this format. A free return preparation utility was launched, so that small deductors would not have to incur a cost in buying software. A platform independent file validation tool was made freely available, so that filers could verify their returns before submission.
4. **Return Acceptance:** The filers could either upload the returns directly to the TIN system on the internet or submit the return to any of the TIN facilitation centres across the country.
5. **Upload of challan details by banks:** ITD also prescribed a standard ASCII text-based file format for upload of challan details to TIN. A platform independent file validation utility for challan files was provided to the banks. Banks were provided the flexibility to upload the challans through leased line connections that they had with NSDL for depository operations, or use dial-up PSTN/ISDN links, or use the internet.

This approach is being followed for the implementation of GST, where *The IT Strategy for GST was defined and accepted within Government even before the NIU was selected. The report of the Working Group on Establishing a National Treasury Management Agency*[1] *and the UIDAI Strategy Overview*[2] *are also examples of Mission Strategy Documents that describe the solution architecture at a high level.*

6.2.2. *Structured change management*

Business process re-engineering (BPR) is essential to the success of an IT project. When a large number of organizations and disparate user segments are involved, it is important to phase the re-engineering. Changes that are most critical for efficiency can anchor the transformation process. A structured change management process should be put in place, so that the process is incremental. A principle of least surprise to the user, so that minimal change in user behaviour is required, is a good principle to guide the change management process. Box 6.1 describes an example from TIN.

6.2.3. *Reflection of policy changes in IT systems*

Changes in policy should be accompanied by the corresponding changes in IT systems; the two should go hand-in-hand. For projects that depend on mission-critical IT systems, if policies cannot be implemented using the IT system, it may be difficult to enforce

[1]Establishing a National Treasury Management Agency: http://finmin.nic.in/reports/Report_Internal_Working_Group_on_Debt_Management.pdf

[2]The UIDAI Strategy Overview: http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf

Box 6.2: Interoperability among depositories

Depositories are established under the Depositories Act, 1996. Initially, there was only one depository, NSDL. Over time, as the concept was accepted, and markets took off, CDSL (another depository) was created. Even though NSDL started out as the only depository, competition emerged over time. The fact that the Securities and Exchanges Board of India (SEBI) required interoperability among various depositories ensures that the customers and the ecosystem are not affected when competing depositories are created.

them practically. Thus, when a change in policy is planned, the teams responsible for the IT systems should be consulted. The policy change should then be announced when the modifications in the IT system have been completed.

6.2.4. *Data quality*

As the saying goes "garbage in, garbage out"; an IT system is only as good as the data it consumes. The system design should have a self-cleaning mechanism. For example, the UIDAI proposes to authenticate the identity of a resident based on data they have provided during enrollment. The system is self-cleaning, because it is in the resident's interest to ensure that the system has correct data, in absence of which he cannot authenticate his own identity. Similarly, TIN has seen a gradual increase in data quality over time, as taxpayers realized the benefits of electronic filing and electronic payments.

Further, clean data can be ensured by standardisation of processes, matching and verifying information in workflows, simple and well defined open data formats, electronic payments and processing, instant feedback to customers, incentives for compliance, and penalisation for non-compliance. It is through incentives that data quality can be managed, rather than micromanagement of stakeholders.

6.2.5. *Vendor neutral solution*

The solution architecture should be vendor neutral. Open standards should be adopted and open source should be used as prudent. In the case that specialised software components are used, the project should define an open standard and require vendors to comply. Multiple vendors can also be selected for such components. Issues relating to openness are discussed further in Chapter 7. It is for this purpose that both, the teams within Government and in the NIU, should include technology experts. A vendor neutral solution architecture also makes it easy to change NIUs or vendors if necessary. A credible threat of migration also ensures competitive pricing.

6.2.6. *Interoperability and multiple providers*

Interoperability among multiple service providers is essential to foster competition in the long run. This can only be achieved if interoperability is built into the system architecture from the outset. Projects that are implemented with NIUs essentially establish natural monopolies in the early stage. Once the requirements are well understood and the ecosystem has formed, there may be justification for competing firms. The example from depositories (Box 6.2) illustrates this point quite well.

6.2.7. *A platform strategy*

A large complex IT project touches a number of stakeholders. It is desirable that such projects employ a *Service Oriented Architecture* in their design. This makes it possible for

Box 6.3: A platform strategy in banking

A bank account is a great example of a platform strategy. A bank keeps a bank account in its core banking platform. This account may be accessed in a number of ways:

1. At the bank branch
2. Through mobile phones using m-banking
3. Through phones using IVR systems and call centres
4. Through the internet using computers, smart phones, and tablets
5. Through ATMs
6. Through debit cards
7. By payment processors to enable merchant transactions
8. By billers for the purposes of automatic billing

If bank accounts were not designed following a platform approach, it would not have been possible to access them through so many channels.

an ecosystem to evolve around standards and services provided by Government. The example of open file formats published by NSDL for e-Returns and e-challans in TIN (Box 6.1) are a good example here. It ensured that the end customer had multiple options to prepare returns. There was no lock-in of a particular software or service provider. Many independent software providers could create new software bringing in competition. At the same time, existing financial accounting software packages could support the new file formats effortlessly. An example from banking is described in Box 6.3.

6.3. Essential public goods

Almost all projects within Government, and the citizens at large will benefit from the essential public goods of connectivity and payments. The Group recommends that Government should make it a top priority to provide connectivity and banking facilities ubiquitously.

6.3.1. *Connectivity*

The Group's conceptualisation of a platform approach to service delivery entails that at the front-end, the data entry and retrieval architecture must be real-time and ubiquitous. In order to enable this, data connectivity at the front-end is critical. The front-end would include Government offices in tier 3 and tier 4 locations as well as Local Governments in rural locations for services such as e-procurement and payroll. For services such as TIN, PAN, and other Government-to-citizen services, the front-end would also include non-Government facilitation centers.

Connectivity in the country has improved by leaps and bounds. The Government has launched various initiatives to ensure last mile connectivity across the country. The recent acceptance of Aadhaar for satisfying proof of identity and address for all telecom connections by Department of Telecommunications will also ensure greater telecom inclusion[2].

[2]Aadhaar as proof of identity and address for telecom connections: http://uidai.gov.in/images/FrontPageUpdates/2011117_114142_telco_notification.pdf

6.3.2. *Banking system interface*

For all services that entail payments to citizens, the last mile interface is the weakest link. An efficient payments and transfers system warrants bank connectivity to every individual and institution, including those in remote rural areas. In the absence of bank accounts, payments have to be effected via an intermediary, which in turn creates room for leakages. With a universal bank account, it can be mandated that payments are made directly into bank accounts. In order to achieve this vision of all payments being universally routed through a bank account, the following are proposed:

1. **Account opening:** Access to bank accounts should be universal. Although the KYC guidelines are largely enabling, more effort in account opening needs to be undertaken. The recent acceptance of Aadhaar as proof of identity and address for opening bank accounts can help accelerate financial inclusion[3]. In the absence of a bank account for every individual, the ability to accurately ascertain individual level outcomes of payments made is not there.
2. **Unique identification of individuals and firms:** We need to minimise errors in identifying individuals (as beneficiaries under various schemes) and firms and ensure foolproof ways for transactions to be authenticated. Dovetailing efforts with the Aadhaar initiative can ensure that payments can be sent electronically by various Governments directly to beneficiaries on the basis of their Aadhaar using an *Aadhaar payments bridge*. Further, microATM and mobile-based person-to-person payments can be simplified by giving concrete shape to the approved framework of the *Inter-Ministerial Group for delivery of Basic Financial Services* [4]. For firms, the PAN has emerged as the unique identifier. All submissions by individuals and non-individuals that involve money transfer and payments should be made electronically and they should be authenticated and validated immediately, to the extent possible.

The Government should closely work with all stakeholders to define a uniform banking interface for Government, so that inter-Government payments may be tightly integrated with internal processes within Government.

[3] Aadhaar as proof of identity and address for opening bank accounts: http://uidai.gov.in/images/FrontPageUpdates/notification_regarding_aadhaar.pdf

[4] Report of the Inter-Ministerial Group for delivery of Basic Financial Services: http://www.mit.gov.in/content/Government-approves-framework-provision-basic-financial-services-through-mobile-phones

7 Openness

7.1. Background

Openness should be an integral part of Government projects. This chapter refers to openness of technology. Openness in technology can refer to the open standards, open data, and open source. The project management team should actively pursue openness at all stages of the project implementation.

Openness is a two-way street. On the one hand, Government, as the producer of public goods funded by taxpayers should define open standards, and release open data in open file formats, along with open source software to the extent possible. On the other hand, the use of open standards, open data, and open source within large complex IT projects brings down costs, leads to higher competition, and increased transparency in implementation.

The Mission team within Government should be committed to the principle of openness to the extent possible. The Department of IT has also released a *Policy on Open Standards for e-Governance*[1], which can serve as a guide for openness.

7.2. Open standards

The use of open standards in the design and implementation of open standards is highly desirable in IT systems. Multiple vendors provide competing solutions that can be used interchangeably with open standards. For example, all major database vendors provide databases that can be used interchangeably. However, most vendors will also provide proprietary extensions that lead to vendor lock-in. The system design must be done carefully, fully adhering to open standards.

While Department of Information Technology notifies national policies on standards from time to time, a project should publish domain specific open standards to cultivate an ecosystem. It is important to note that these new open standards are not devised in a top-down approach, but are created out of necessity, and from practical experience. Examples from UIDAI on publishing new open standards are mentioned in Box 7.1.

[1] Policy on Open Standards for e-Governance: http://egovstandards.gov.in/approved-standards/egscontent.2010-11-12.9124322046/at_download/file

Box 7.1: Open standards at UIDAI

The UIDAI has deployed open standards in the design and implementation of its IT systems, as well as released open standards relevant to its core mission. For the core mission of UIDAI of collecting demographic and biometric data of residents to issue Aadhaar numbers, the following standards have been published:

1. **Demographic data standards:** The UIDAI published standards for the collection and storage of demographic data in the **Demographic Data Standards and Verification Procedure Committee Report'**, under the chairmanship of Mr. Vittal[a]. This includes standardization of the data fields to collect and store name, address, date-of-birth, and gender.
2. **Biometric data standards:** The UIDAI published standards for the collection and storage of biometric data in the **Report on Biometrics Design Standards for UID Applications**, under the chairmanship of Dr. Gairola[b].

[a]Demographic Data Standards and Verification procedure Committee Report: http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf

[b]Report on Biometrics Design Standards for UID Applications: http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

7.3. Open data

The Government, as a producer of public goods should release data in well-defined formats electronically, when possible, as prescribed by the *Right to Information Act, 2005*. Open data can become a foundation for a number of transformational IT projects in Government. Innovative firms and individuals can combine various types of data to glean new information that may not have been possible from the individual datasets.

Open data is already released by various Government agencies. One example is the Department of Statistics, under the Ministry of Statistics and Program Implementation, which releases various statistics based on surveys and compiling the national accounts. This can be emulated throughout Government. There is a need of a much greater scale of release of unencumbered data, placed into the public domain, of information created within Government.

There can be economic data, map data, census data, pollution data, water data, soil quality data, climate data, PIN code data, administrative boundaries data, health data, Government accounts data, etc., which is released by the relevant ministries. Early international experiences[1] of releasing open data using open file formats have resulted in mashups, which combine data from multiple sources and present it in ways that yield new insight, have been encouraging.

Open data can become the foundation of a transparent and accountable Government. Thus, it is important that the designers of IT systems keep open data in mind. This point is elaborated further in Chapter 9.

7.4. Open source

Open source refers to providing the source code of a computer program in the public domain, for others to examine and use. Today, entire operating systems, desktop software, office productivity suites, and server software are examples of software that are available as open source.

[1]Release of open data using open file formats: US (http://www.data.gov) and UK (http://data.gov.uk).

There are some who believe that in cases where open source software is available, no commercial software should be used. This can sometimes be counter-productive, since there may be cases when commercial software is better suited than the open source versions. It is not a good idea to force the use of specific software of any type; instead, the focus should be on adopting open standards, and using open source as prudent.

The Mission Execution Team in Government should also ensure that components of a project that may be reusable by other projects are released as open source software. While some may argue that the Government should open source the entire project, the Group recognizes the intellectual property of the NIU. The committee also recognizes that it may be counter-productive to the business planning and profitability of the NIU to release all source code as open source. The Government and NIU should work together from the early phases of the project in deciding what components can be open sourced.

In summary, there are enormous benefits from both using open source that is available off the shelf, from participating in the development process of existing open source software so as to extend existing open source systems into superior functionality (while feeding these extensions back into the public domain), and from releasing new open source systems. Every IT system in Government will benefit from pushing in all these three directions. At the same time, these three approaches should not become an inflexible dogma.

7.4.1. *An Open Source Foundation*

Today, the major impediment to Government projects releasing source code is the lack of a proper process for open-sourcing applications and housing them. The existence of an open source foundation, along with a well-defined process to release open source software can help drive the creation of an effective e-governance software stack.

The Group suggests that the Government in partnership with concerned stakeholders should set up an open source foundation[2] to host open source software released by Government projects.

[2]Some examples of open source foundations are the Apache software foundation (http://www.apache.org/foundation/) and Eclipse foundation (http://www.eclipse.org/org/).

8

Information security

8.1. Background

As the use of mission-critical IT systems becomes widespread within Government, the growing connectivity between these information systems, the Internet and other infrastructure, create opportunities for increasingly sophisticated attacks on such systems. Such attacks may be made by individuals, non-state players, as well as by hostile Nations. It is therefore essential to ensure that any disruptions of critical Government information systems are contained and managed effectively to minimize their impact. The security team for important projects must be best in class, and the security solutions must always be cutting edge at all times.

Information security breach may include consequences such as financial losses, systems being rendered unusable, intellectual property theft, damage to the organization's brand and reputation, and legal exposure or lawsuits, among others. These consequences may be on account of: confidential records or sensitive information being compromised or being made unavailable, identity theft due to customer or employee information being stolen, modification or alteration of the operating system programs, software applications, files, data etc., or crippling of infrastructure such as networks and applications.

These concerns are heightened when aspects of national security also come to the fore, an example of which is described in Box 8.1.

8.2. Institution-wide support for information security

Security is widely regarded as a hygiene factor which comes to fore only in times of disaster, while in organizations that manage security well, the ownership of security vests at the highest levels of governance. Without the visible support of senior management it may not be possible to actually implement the required security framework, ensure compliance by users and elicit co-operation.

Implementing security is often considered a one-time activity, which is effectively discharged when funding approvals are accorded for a technology stack. It is often perceived that having a set of information security tools will ensure adequate protection for a reasonable period of time. Even as implementing teams close all the known

Box 8.1: Geo-political nature of attacks on IT systems

Stuxnet is an Internet worm that infects Microsoft Windows computers. It primarily spreads via USB sticks, which allows it to get into computers and networks not normally connected to the Internet. Once inside a network, it uses a variety of mechanisms to propagate to other machines within that network and gain privilege once it has infected those machines.

Stuxnet doesn't actually do anything on those infected Microsoft Windows computers, because they are not the real target. What it looks for is a particular model of Programmable Logic Controller (PLC) made by Siemens. These are small embedded industrial control systems that run all sorts of automated processes: on factory floors, in chemical plants, in oil refineries, at pipelines, and in nuclear power plants.

If it does not find one, it does nothing. If it does, it infects the PLC using what was then an unknown and unpatched vulnerability in the controller software. The changes made by Stuxnet are very specific, targeting a specific group of PLCs, leading many to believe that Stuxnet's authors had a specific purpose in mind.

Stuxnet does not act like a criminal worm. It does not spread indiscriminately. It does not steal credit card information, or account login credentials, nor does it herd infected computers into a botnet. It does not threaten sabotage, like a criminal organization intent on extortion might; it performs sabotage. The damages due to Stuxnet have also been compared to a military operation.

Analysis of the worm suggests that it was expensive to create. It is estimated that a team of talented programrs developed it over a period of six months, in a laboratory setting.

Source: Forbes magazine (Oct 2010), New York Times (Jan 2011)

weaknesses and gaps, intruders develop new and more sophisticated methods of attacks. Thus the information security landscape is dynamic in nature and techniques that worked at one point may not suffice for the current year. Often a regular high level review and monitoring framework is not in place, leading to a reactive rather than proactive approach to information security.

Within the NIU framework suggested in this report, security should be given utmost importance by the Mission Team within Government, and by the management team at the NIU. A Chief Information Security Officer (CISO) should be appointed who is empowered and fully responsible for all aspects of information security: technology, processes, and people (Figure 8.1).

Security must be part of the ethos of the organization, and can only be achieved when the entire organization (right from senior management to field personnel) is geared for it. This requires training and awareness on basic facts about information security (strong passwords, how systems are hacked, denial-of-service attacks, social engineering, de-mystifying jargon etc.) all levels.

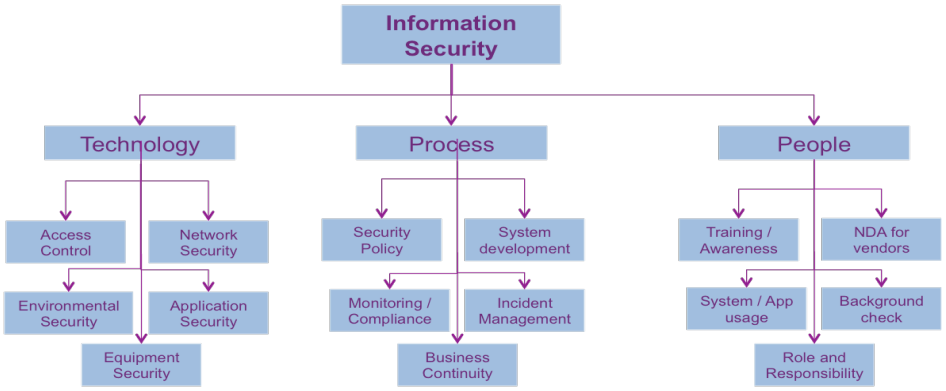
Getting certified for various standards, and audited by independent security auditors help provide the CISO with a basic understanding of the level of security within the organization. It is essential, that as problems are identified, not only the symptoms are treated, but the root cause of the problems are also identified and processes are put in place to avoid them in the future.

8.2.1. *Certification*

Various international standards and best practices can customized to define a comprehensive certification framework:

1. The ISO 27001 is a formal management system that brings information security under explicit management control.
2. ISO 15048 (Common criteria) provides a basis for verifying security functionality of IT products as well as ensuring that they are free of trap-doors etc.

Figure 8.1: Controls for information security



3. BS 25999 provides guidelines for the implementation of disaster recovery and business continuity management framework.

Some of these certifications are expensive to achieve, and although they provide a broad framework to evaluate security of an IT system at large, they are by no means sufficient.

8.2.2. *Audits*

Audits are performed by an independent third party, and thus provide an independent evaluation of the security of an IT system. The scope of audits may include:

1. **Technology review:** which covers all the technology components of the IT project such as
   (a) **Ethical hacking:** Vulnerability assessment and Penetration testing of the network
   (b) **Application Security:** Application security audit to identify known vulnerabilities and source code review:
   (c) **Design Review:** Review the IT architecture from security point of view and identify single point of failure.
2. **Process Review:** Review should cover all the process related to security adopted by the IT project such as change management, Log review, access control etc
3. **Third party review:** Review the security controls deployed by the third parties on the Government data/information

8.3. Solution architecture and information security

Security should be an integral of the solution architecture, and not an afterthought. The following ideas can help guide the design of the solution architecture from a security perspective:

1. **Identity, access and entitlement management:** Providing authentication and authorization services are the core objectives of this control. It ensures that right people have access to right resources. Having access to fewer resources than necessary for a particular task hampers productivity, while access to more resources than necessary introduces risk.

2. **Host access management:** A dedicated host access management solution greatly strengthens the security of mission-critical servers. Such a solution can improve security, simplify and reduce the cost of server administration, and provide significantly improved audit capability needed to address regulatory compliance and security best practice requirements.
3. **Data encryption:** Encryption of data ensures that information stored in the system (referred to as plaintext) is transformed into an unreadable form using an algorithm (called ciphertext) for anyone except those possessing special knowledge, usually referred to as a key. This helps in providing assurance of confidentiality of information, even in cases of unauthorized access.
4. **Data hashing:** Hashing of data ensures that any alteration to even a bit of data drastically changes a special fixed length code called hash, created from the original data stream. This helps in providing integrity assurance to trusted set of information. Passwords and other sensitive information are often stored only as hashes, so that access is granted only if the generated hash matches a stored hash.
5. **Data classification and data loss prevention:** : Data Loss Prevention (DLP) systems are designed to detect and prevent the unauthorized use and transmission of confidential information. DLP increases the effectiveness of existing controls by minimizing inadvertent and malicious data loss, and will empower the organization to comply with various data protection regulations. It provides a customizable level of control at critical areas throughout the Organization — at the endpoint, the network, the message server and for stored data.
6. **Transaction audit:** It is imperative to analyse transactions for anomalous behaviour as well as to collect sufficient forensic data for each transaction so as to enable the monitoring engine to establish the difference between a normal transaction and a fraudulent transaction.
7. **Interaction security:** At interaction level, it is necessary to ensure that security is taken care of at each interaction point that includes people-system interaction as well as system-system interaction. All workflows and business processes should be developed keeping security in mind. All the interactions must be under audit and audit trails should be secured. There must be clear and specific security policies that define roles and responsibilities for all interaction in the organization.

8.4. Threat to information security from insiders

Projects that depend upon mission-critical IT systems may have a number of employees, and an order of magnitude larger number of customers. Employees are given privileges within the system to enable them to carry out their daily functions. It has been observed in a number of cases that security is often at risk due to insiders having authorized access, but use this authority in ways that are malafide. A security-conscious design of the solution architecture, combined with a dedicated CISO and security team are essential to combat not only external security threats, but also security threats emanating from within the organization.

8.5. Legal framework governing information security

In order to deal with information security crimes, the Information Technology Act, 2000 (hereinafter, referred to as IT Act, 2000) was passed, covering inter alia:

1. Legal Recognition of Electronic Documents
2. Legal Recognition of Digital Signatures

3. Offenses and Contraventions
4. Justice Dispensation Systems for Cyber crimes

The Information Technology Act, 2000, was further amended through the Information Technology Amendment Act, 2008 (ITAA 2008). ITAA 2008 addresses the emergence of various types of cyber-crime, such as identity theft and the creation of malicious computer code. This Act provides the legal framework to promote IT in the country and:

1. Empowers Government to accept filing, creating and retention of official documents in the digital format.
2. Provides for legal effect, validity and enforceability of electronic records.
3. Provides for the authentication and origin of electronic records and communications through digital signature.
4. Provides a more exhaustive coverage of cyber crimes in law.

Some other Acts (and their associated regulations) which Government organizations are required to comply with (apart from the statutes governing the concerned Departments), include Indian Evidence Act 1872, Official Secrets Act 1923, Indian Copyright Act 1957, and Right to Information Act, 2005.

8.6. National level considerations

The Group has suggested a security-conscious design of the solution architecture, a dedicated security team headed by a CISO, and basic security training for all employees to tackle internal and external security threats to a project. There is merit in sharing information and learnings across various Government projects, and co-ordinating across projects in case of large-scale attacks on various systems. The security teams of individual projects should integrate with existing agencies set up by the Government such as CERT-In[1], and with other frameworks that evolve over time.

[1] Cert-In (http://www.cert-in.org.in/) is the national nodal agency for responding to computer security incidents as and when they occur.

9

Accountability, transparency, and self-corrective forces

9.1. Background

The passage of the *Right to Information Act, 2005* (RTI Act) that guarantees citizen access to nearly all Government information not deemed to be critical for national security, has caused a sea change in how citizens interact with, and monitor, Government.

If deployed effectively, information technology has the potential to serve as a powerful tool to bring about transparency and accountability of Government services. Yet, increased transparency and accountability is by no means a guaranteed outcome of a Government IT project. IT projects which are not designed with an explicit objective of increasing transparency, which lack a clear channel through which the IT system will increase transparency, or which fail to take into account the interests of the various stakeholders in the IT system will fail to increase transparency or accountability.

9.2. What to share

The Group recommends that designers of Government IT systems take a pro-active stance in deciding which information to share publicly. As a large share of the information collected by the Government must be provided according to the provisions of the RTI Act, proactively sharing data can obviate the need for responding to RTI requests on an individual basis, while also making it easier for citizens to access this data.

9.3. Solution architecture and transparency

The architecture of an IT project must be designed keeping a transparency portal in mind. A large IT project produces large volumes of data daily. If a transparency portal is designed as an afterthought, the end result may be lack-lustre.

Typically, the same software architecture for data warehousing, data mining and business intelligence required within an IT project for policy support and analysis can

also support the operations required for a transparency portal. Even though a portal is created with basic analytical capabilities, all the data should be made available in simple, well-defined, machine-readable formats.

9.4. Self-corrective forces

A transparency portal for an IT project in Government works as a positive feedback loop. The fact that such a portal is implemented, means that analytics about the performance of the project are generated immediately. As a result, any deviation from expected behaviour is detected quickly and rectified.

In case such a portal is not well thought out, potential problems may manifest themselves much later, and may turn out to be difficult to fix. A transparency portal leads to monitoring and feedback at various levels: within the service provider, within Government, and by citizens at large. The NREGA MIS portal is an example of such a transparency portal (Box 9.1).

9.5. Contact centre

The contact centre closes the feedback loop of self-corrective forces. It establishes multiple channels of communication with all stakeholders, including end-users, for purposes of gathering information and reporting grievances. An effective contact centre is tightly integrated with the IT systems, so that queries and complaints can be dealt with effectively, and information is recorded and updated on a real-time basis. Some of the key features of such a contact centre[1] are as follows:

1. Provide services in multiple languages
2. Provide inbound channels of communication such as voice, fax, letters, e-mail, and a web portal
3. Provide outbound channels such as voice, fax, letter, e-mail, and SMS messages
4. Available during working hours, or on a 24-by-7 basis, depending upon the nature of the project
5. Deploy key technologies such as a Customer Relationship Management application (CRM), Interactive Voice Response System (IVRS), Automatic Call Distribution (ACD), Computer Telephony Integration (CTI), call logging, quality management system, email response system, and scanning solutions for letters and faxes.

9.6. Crowd-sourcing

Enabling citizens and beneficiaries of public schemes to directly provide feedback using web and mobile phone-based platforms is a powerful way of involving citizens in improving public accountability. It unlocks the potential of collective wisdom[2]. In addition, the ability to combine spatial and financial data can provide very powerful maps to track the progress of various initiatives and schemes.

[1] An example of a contact centre from UIDAI: http://uidai.gov.in/UID_PDF/Front_Page_Articles/Recent_Tenders/CONTACT_CENTERS/RFP_for_setting_up_and_operating_contact_centers_for_UIDAI_Ver3.pdf

[2] Examples of technology platforms that have successfully used crowd-sourcing are Ushahidi, Transparent Chennai, Environment Sustainability Index, Pollution Index, and e-Government's foundation projects.

Box 9.1: NREGA MIS portal

The National Rural Employment Guarantee Act (NREGA) aims at enhancing the livelihood security of the people in rural areas by guaranteeing hundred days of wage employment in a financial year, to a rural household whose members volunteer to do unskilled manual work. The Act contains specific provisions for public accountability. Based on the statutory directives, the guidelines stipulate a three-pronged strategy for public accountability: proactive disclosure, social audit, and a grievance redressal mechanism.

The Ministry of Rural Development has set internal and external systems to closely monitor NREGA both physical and financial performance of States.

1. **Management Information System (MIS):** A web enabled public MIS[a] hasbeen developed. The village level household database has internal checks for ensuring consistency and conformity to normative processes. All critical parameters get monitored in public domain: a) workers' entitlement data and documents such as registration, job cards, muster rolls, (b) shelf of approved and sanctioned works, works under execution, measurement (c) employment provided (d) financial indicators including wage payment. Till FY 2008-09, 6 crore Job Cards and 1.2 crore muster rolls have been placed on MIS.
2. **Statutory institutional mechanisms:** At the national level, a Central Employment Guarantee Council has been set up with the statutory mandate of monitoring and reviewing the Act. The Ministry also invited the CAG to conduct a concurrent audit of the program in the very first year of implementation to assess gaps in program implementation by States, so as to initiate remedial measures at an early stage.
3. **Other mechanisms:** Other mechanisms include National Level Monitors and Area Officers, and officials of the ministry who undertake annual field visits, quarterly performance review with States. A Professional Institutional Network (PIN) has also been constituted for steady, sustainable interventions that enhance the quality of the program. These institutions will conduct impact assessment, concurrent monitoring and appraisal, research, capacity building to identify both good practices factors that have or will limit the optimal performance of the scheme. Currently, the network has 18 member institutions, including Indian Institute of Technology (IITs), Indian Institute of Management (IIMs), Administrative Staff College of India (ASCI), Indian Institute of Forest Management (IIFM), Agriculture Universities and other professional institutions. In its first phase, 13 institutions have conducted an NREGA appraisal.

[a]NREGA MIS portal: http://www.nrega.nic.in

9.7. International experiences

Various Governments are now leveraging the capabilities of IT platforms to democratize public data, to drive innovation, and provide transparency in the operations of Government. Some of the notable examples of portals that aggregate Government data and make it available in common data formats are as follows:

1. **USA:**
   (a) The Federal Funding Accountability and Transparency Act (FFATA) of 2006 requires that the Office of Management and Budget (OMB) establish a single searchable website, accessible to the public at no cost, which includes for each Federal award: the name of the entity receiving the award; the amount of the award; information on the award including transaction type, funding agency, etc; the location of the entity receiving the award; and a unique identifier of the entity receiving the award. http://USAspending.gov was first launched in December 2007 to fulfill these requirements.
   (b) A primary goal of http://Data.gov is to improve access to Federal data and expand creative use of those data beyond the walls of Government by encouraging innovative ideas (e.g., web applications). Data.gov strives to make Government more transparent and is committed to creating an unprecedented level of openness in Government.

(c) http://ITDashboard.gov is a website enabling federal agencies, industry, the general public and other stakeholders to view details of federal information technology investments. The purpose of the Dashboard is to provide information on the effectiveness of Government IT programs and to support decisions regarding the investment and management of resources. The Dashboard is now being used by the Administration and Congress to make budget and policy decisions.

2. **Brazil:** The Government of Brazil provides a transparency portal for expenditure data at http://www.portaldatransparencia.gov.br/. This Transparency Portal was created in November 2004 for the purpose of making it possible for public managers and citizens at large to follow up on the financial execution of all programs and actions of the Federal Government more easily. The information available in it includes: funds transferred by the Federal Government to States, municipalities and the Federal District; funds directly transferred to citizens; direct spending of the Federal Government with procurement or contracts for projects and services, including the spending of each agency with per diems, office supplies, equipment, projects and services; as well as spending through Payment Cards of the Federal Government.
3. **UK:** The Government is releasing public data to help people understand how Government works and how policies are made. Some of this data is already available elsewhere, but http://data.gov.uk brings it together in one searchable website. Making this data easily available means it will be easier for people to make decisions and suggestions about Government policies based on detailed information. There are currently over $5,400$ datasets available, from all Central Government departments and a number of other public sector bodies and local authorities.

The enabling framework for an Expenditure Information Network (EIN) is slowly coming into place. There is a need for an effective monitoring, evaluation and accounting system for the large sums of money that are disbursed by the Central Government to State Governments, district level agencies and other implementing agencies. While there are various stand-alone efforts in this direction, there is as yet no consolidated Expenditure Information Network (EIN). This Group recommends details of the proposed EIN in Chapter 13.

10 Protection of the individual

10.1. Background

As IT systems become commonplace in governance, issues related to the protection of the individual's right to privacy come to the fore. With paper records, the risk of unauthorized access of large quantities of data has been limited due to the difficulty of aggregating and accessing the data. When data is stored in electronic format, the risk is greater. Data protection provisions already exist in existing legislations like the Information Technology Act, 2000.

The Department of Personnel and Training (DoPT) is currently engaged in preparing a legislative framework on data protection, which would also address issues pertaining to an individual's data in the context of IT systems[1]. These recommendations may serve as useful guidelines for designers of IT systems until such a date that formal legislation on privacy is passed.

10.2. Solution architecture and privacy

Just as the solution architecture of a project should be designed taking security (Section 8.3) and transparency (Section 9.3) into account, it should also be designed from the ground up to support privacy of end-users. The privacy framework for a project should be defined early on, which translates the legislation on privacy into implementable rules for IT systems.

10.2.1. *Personal identifiable information*

The design of the solution architecture should ensure that any Personal Identifiable Information (PII) is stored safely, and access is carefully monitored. To the extent possible, workflows should be designed so that access to PII is avoided. Also, PII should be stored in encrypted form, and separately from other data. Separate access controls may be defined, with strict access control, monitoring, and logging of all access to PII data.

[1] Approach paper for a legislation on privacy: http://persmin.gov.in/WriteReadData/RTI/aproach_paper.pdf

Stringent penalties must be in place to address the issue of unauthorized access of personal data by outside agencies as well as by personnel within the organization. Strict protocols and processes must be in place to detect such access in order that they are dealt with swiftly and in a deterrent manner. This is not only desirable from a privacy perspective, but also from a security perspective.

10.2.2. *Anonymization*

Anonymization of data is an important aspect of privacy. Data should be carefully anonymized when released publicly, or when shared with other organizations that do not require access to PII, as allowed within the data protection and privacy framework. Careful thought should be given to anonymization, since naive approaches to de-identifying data are prone to attacks that combine the data with other publicly available information to re-identify individuals. The concept of k-anonymity has been defined in the academic literature on privacy, where each record within the system is at least indistinguishable from $k-1$ other records in the released dataset. Thus, privacy is protected by guaranteeing that every released record will relate to at least k other individuals in the dataset, even if the records are directly linked with other external information. Translating this theory into practice may not be easy, but designers of the solution architecture should try to approximate such concepts in their design to the extent possible.

10.2.3. *Data retention and usage policy*

Data retention and usage policies should be well-defined, especially for PII. It may be necessary to retain transaction logs for long periods of time for purposes of analysis and research, but PII should be scrubbed from these logs after a pre-defined period. In case the legal framework of the project provides for it, an individual should be able to access data stored in the IT system about themselves, after appropriate authentication of their identity.

10.3. Balancing the right to privacy with public interest

The right balance between the individual's right to privacy and the larger public interest should be achieved by the data protection framework. While personal information relating to the individual must be strictly protected from unauthorized access, there may be a need for Government agencies to access or share this data for purposes of national security, economic offenses, tax evasion and other specified circumstances. Hence, authorized sharing of information under specified circumstances, ipso facto, should not be considered as a violation of an individual's right to privacy. However, detailed processes, systems and guidelines need to be put in place to ensure that authorized access and sharing is within the parameters set by law.

Part III

Recommendations for Ministry of Finance projects

11

Goods and Services Tax

11.1. Introduction

The Goods and Services Tax (GST), which will replace the State VAT, Central Excise, Service Tax and a few other indirect taxes will be a broad-based, single, comprehensive tax levied on goods and services. It will be levied at every stage of the production-distribution chain by giving the benefit of Input Tax Credit (ITC) of the tax remitted at previous stages. GST is based on a destination-based taxation system, where tax is levied on final consumption. It is expected to broaden the tax base, foster a common market across the country, reduce compliance costs, and promote exports. The GST will be a dual tax with levy by both Central and State tax administrations on the same base. The GST demands a well-designed and robust IT system for realizing its potential in reforming indirect taxation in India. The IT system for GST would be a unique project, which will integrate the Central and State tax administrations.

11.2. Public policy challenges

11.2.1. *Placement of tasks*

11.2.1.1. *Governance bodies*

The following governance bodies have been constituted for realizing the vision of GST and implementing it:

1. The Empowered Committee of State Finance Ministers (EC) set up to work with the Central Government to lay down the features of GST and oversee its implementation.
2. The Joint Working Group (JWG) constituted by the Empowered Committee in consultation with the Central Government to prepare the roadmap for GST implementation.
3. The Empowered Group on IT for GST (EG-IT) formed in July 2010 for devising the IT strategy for GST and monitoring its implementation.

11.2.1.2. *GSTN as the NIU*

The EG-IT has recommended setting up of an NIU — Goods and Services Tax Network (GSTN), for managing the IT systems for GST implementation, including the Common GST Portal. GSTN will perform the following functions:

1. Provide common infrastructure and services to Central and State Governments
2. Ensure integration of the Common GST Portal with existing tax administration systems of Central and State Governments
3. Build efficient and convenient interfaces with tax payers and tax administrators
4. Facilitate, implement and set standards for providing common GST services to the Central and State Governments
5. Carry out research, study global best practices and provide training to the stakeholders.

The Group endorses the above approach and recommends that the GSTN should be set up as an NIU as envisaged in Chapter 1 of this report.

11.2.2. *Incubation of the project*

The EG-IT has suggested that the GSTN project may be incubated within NSDL and this suggestion has been generally accepted. The preliminary work of conducting a proof-of-concept is being undertaken by NSDL and it has been planned to run a GST pilot with selected State Governments participating in it along with the CBEC. The Group commends this approach and recommends that the infrastructure for the GSTN should be based on latest technology and ring fenced, so that whenever the *spin-off* takes place, the GSTN infrastructure is smoothly transferred to the proposed NIU being set up as GSTN.

The IT strategy document for GST prepared by the EG-IT, which defines the contours of the IT implementation in respect of the GST Common Portal and its interface with all stakeholders, could form the basis for taking forward the implementation of GSTN.

11.2.3. *Human resources*

The Group recommends that a dedicated Mission Leader and a dedicated Mission Execution Team be appointed for GST. The NIU for the implementation of GST — GSTN — should be set up with the highest priority.

The Group further recommends that an implementation team, comprising of officers drawn from the CBEC and some of the State Governments (pending the appointment of a full-fledged Mission Team and during the pilot stage) should be set up at the earliest. This team would work along with the teams that would be set up by NSDL for implementing the project. The two teams should together initiate the implementation of the GSTN including such as acquisition of necessary infrastructure, design and development of the application, etc. The personnel selected to man the implementation team should be trained in the tasks mentioned above. Hiring of talent on contract basis should also be explored as necessary. This team should later be part of the Mission Execution Team.

The implementation of GST is based on a substantive change contemplated in the relevant laws and procedures of Central and State Governments. It is essential that the GST Mission Execution Team includes professionals with legal expertise.

11.2.4. *Agreement with NSDL*

The Agreement with NSDL should be drawn carefully and with clarity.It should include aspects such as financials, responsibilities of the Government side and NSDL at the incubation stage, acquisition of infrastructure, development of application software, ownership of source code, spin-off to the NIU, and the process of transfer of assets (both tangible and intangible).

Further, though NSDL is assisting the Government in incubating the GSTN, once GSTN is set up as an NIU, the latter may continue to procure services from NSDL in the initial phases of GST implementation, as it considers necessary.

The GSTN may, as and when it commences its full-fledged operations, adopt a business outcome based, per-transaction pricing model. Even during the period when NSDL is providing such services, a similar approach is recommended.

11.2.5. *Multiple levels of Government*

The Central and State Governments have accepted in principle the setting up of GSTN as an NIU, as a way to align incentives of all stakeholders. The joint ownership of GSTN by all States and Central Government ensures that no stakeholder loses strategic control. GSTN will develop and operate the Common GST Portal, which will have common minimal functionality, but will be customizable and extensible by various Governments.

GSTN will render the following services through the Common GST Portal:

1. Dealer registration (including existing dealer master migration and issue of PAN based registration number)
2. Payment management including payment gateways and integration with banking systems
3. Return filing and processing
4. Taxpayer management, including account management, notifications, information, and status tracking
5. Tax authority account and ledger Management
6. Computation of settlement (including IGST settlement) between the Centre and States
7. Processing and reconciliation of import GST and integration with EDI systems of Customs
8. MIS including need based information and business intelligence
9. Maintenance of interfaces between the Common GST Portal and tax administration systems
10. Provide training to stakeholders

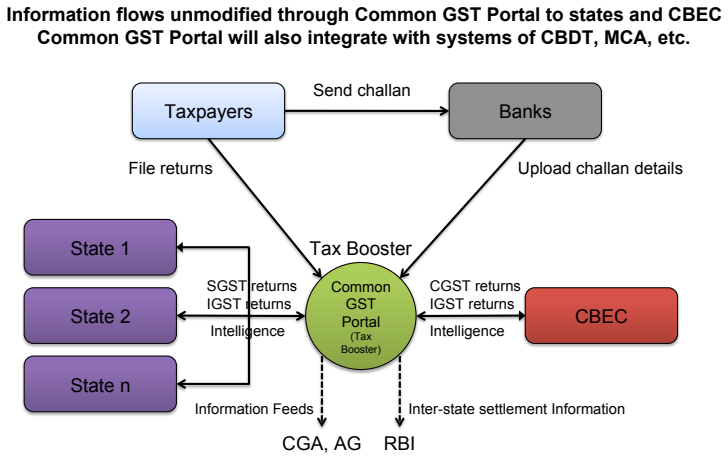
The CBEC and State Governments may design and develop their own applications to meet requirements for effective tax administration such as audit, intelligence gathering, enforcement, and risk management.

11.3. Technology challenges

11.3.1. *Solution architecture for GSTN*

The solution architecture for information flow (Figure 11.1 and funds flow (Figure 11.2 is designed to ensure timely delivery of information through the Common GST Portal, and timely delivery of funds directly through the banking system.

Figure 11.1: GST solution architecture: information flow



The Common GST Portal is simply a pass-through device for information, while enhancing it with intelligence to plug leakages. The taxpayer sends the return with GSTN, which keeps a copy of the return for analysis, and forwards it in near real-time to the respective State and CBEC. The taxpayer pays the actual duty in the bank, which uploads only the challan details into the GSTN. Actual funds never pass through the GSTN.

The Common GST Portal reconciles the returns and the challans. In addition to its pass-through role, the portal would also play two other critical roles:

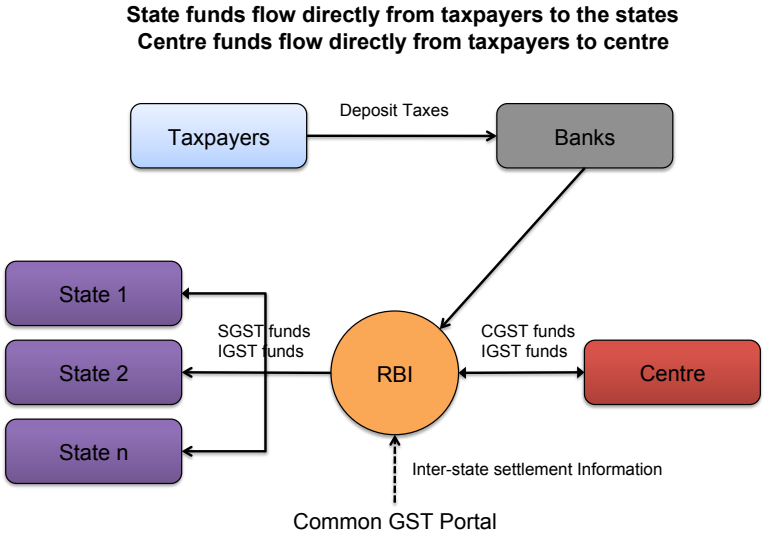
1. It would act as a tax booster, matching the input tax credits in the returns to detect tax evasion. It can also integrate with various other systems at MCA and CBDT for verification of PAN or other corporate information and perform data mining and pattern detection to detect tax fraud. It would send this information as alerts/ reports to the respective tax authorities.
2. It would also compute inter-State settlement, netting IGST across States.

11.4. The way forward

The GST project not only presents several public policy changes, but also requires adherence to tight timelines. In terms of implementation of the IT systems for the administration of the GST, the following important milestones that would facilitate timely implementation should be kept in view:

1. Finalisation of business processes registrations, returns, payments
2. Commencement of GST pilot project by NSDL with identified States and Centre.
3. NSDL to set up core functionalities of common portal in pilot and provide APIs for all stakeholders. Limited testing of APIs by participating stakeholders.
4. Engaging with participating entities for pilot including dealers, banks and other Government agencies.
5. Completing the impact analysis for GST and initiating steps to align existing tax systems at Center and all States for GST. This would include changes to business and IT infrastructure. Timely financial approvals and procurements would also be critical.

Figure 11.2: GST solution architecture: funds flow



6. Evaluation of Pilot Project resulting in iterative review of processes/ IT implementation.
7. Finalisation of detailed project report for actual implementation of GST
8. Attaining clarity on NIU engagement and structure of GSTN.
9. Creation of GSTN and formalising the involvement of NSDL in GST implementation.
10. Finalisation of IGST legal framework and business process.
11. Implementing the stakeholder outreach program
12. Scaling up to GST implementation:
    (a) Administration and organisational restructuring
    (b) Training and testing of applications by tax payers and all tax authorities

The Group notes that the CBEC has set up data centers to run centralized applications for Central Excise, Service Tax and Customs purposes. With the implementation of GST, these and other facilities should be leveraged to the extent possible. An in-depth study (either by an in-house team or by a consultant) of the reusability of the existing ACES project components should be undertaken and necessary steps should be initiated to refashion the same and integrate it with the GST solution.

12

Tax Information Network

12.1. Introduction

Successful tax administration is about making tax compliance painless and tax evasion painful. In order to modernize the systemic processes of tax administration, the Task Force on Direct Taxes, set up by Government of India under the Chairmanship of Dr. Vijay Kelkar, recommended in 2002 establishment of an electronic national Tax Information Network (TIN). Today, this network integrates primary information of tax payments made in designated banks, Tax Deduction at Source (TDS) Returns and information on high value transactions through Annual Information Returns (AIR) into a central database, which gives a 360 degree view of the taxpayer.

Income Tax Department (ITD) established TIN in 2003 through NSDL as a Managed Services Provider model providing the following services:

1. To receive information relating to tax payments coming from banks and enable necessary reconciliations between ITD, banks and accounting agencies in the Government of India
2. To receive TDS returns, digitize the same and enable reconciliation of information in these returns with the payment details received from the banks
3. To collate Information relating to TDS and compile Permanent Account Number (PAN) ledgers reflecting TDS and payment details for each of the taxpayer entities
4. To receive, compile and collate information relating to high value financial transactions coming through Annual Information Returns (AIR)

TIN has helped ITD to ensure that tax credit is given to a taxpayer only against tax reported to Government account. Further, this revised process ow and automation has enhanced convenience in record keeping relating to TDS returns, ling of returns with TDS particulars and has reduced cost of compliance for the taxpayers. The system is designed in a way that it is in the taxpayer's interest to ensure a high level of data quality and compliance. It is reported that the data quality in TIN has dramatically improved over the years, and continues to improve. Thus, TIN has contributed to reduction in leakage, increase in tax base, improvement in process efficiency and transparency, enabled speedy reconciliation, facilitated faster transfer of tax collected to Government and help in data mining to identify trends and making projections.

12.2. Public policy challenges

12.2.1. *Placement of tasks: NSDL as the MSP*

The ITD decided to outsource the technology-centric part of tax collection and TDS data as well as high value financial information on an MSP model to NSDL. The Department could, therefore, focus on its core functions in the areas of policy making, policy administration, tax assessment, and detection of tax evasion. NSDL was engaged for its expertise in data collection and consolidation, rather than establishing the infrastructure in-house. This placement of tasks is similar to that of an NIU, as described in Chapter 1. Outcome based per-transaction pricing was agreed upon, enforced through strict SLAs. Since it also provides for a reasonable return on investment (ROI) to the Service Provider over the tenure of the contract, the Service provider has a continued interest in successful running of the project. The ITD has developed an element of partnership with the service provider, and thus is able to meet its requirement of additional optional services based on changing or upcoming business needs. Automation of the processes and services through TIN has reduced the cost of compliance for the taxpayers, resulting into better voluntary compliance. At the same time, automation of the process of collection and collation of information has resulted into a more effective deterrence against tax evasion.

The Group takes note of this aspect and is of the view that to the extent possible keeping in view the sensitivity of the data, such model could be replicated in other aspects of ITD and other Government Departments, wherein technology driven data capturing processes are entrusted to specialized entities who would enable the processes with none or limited or pre-specified rights towards access and usage of data. Such entities may act as enablers to strengthen the information flow to the concerned departments.

12.2.2. *Human Resources*

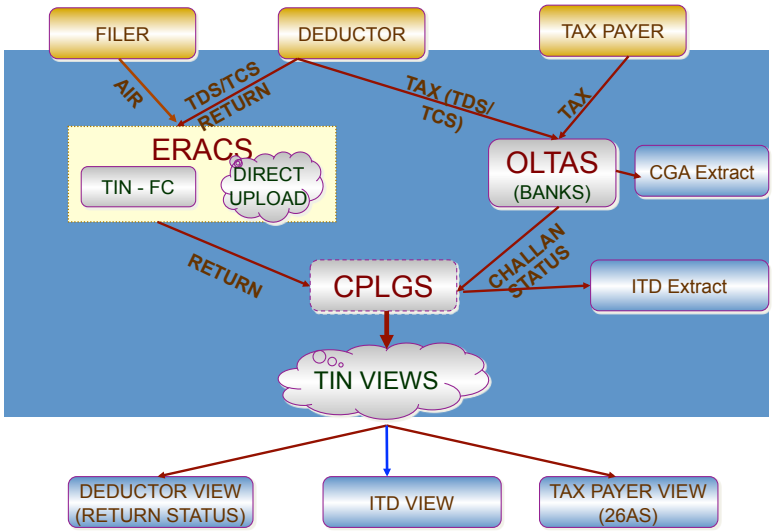
The Directorate of Income Tax (Systems) has acted as the dedicated agency responsible for defining the specifications, contracting with the service provider, getting the project up and running in partnership with NSDL, monitoring and controlling the implementation, and planning change management on the basis of feedback from various stakeholders. An officer in the rank of Joint Secretary (known as Director in the Directorate of Income Tax (Systems)) has played the role of the Mission Leader and he is being assisted by in-house technical staff to supervise this project. Now that the project has reached steady State, the Mission Leader has certain additional responsibilities.

NSDL has separate heads of Department for systems and business operations who are assisted by a team of functional and domain experts. The TIN team has separate process and sub-process owners for various modules like TDS, OLTAS, PAN Ledger Generation, data extraction etc. both in systems and operation areas. NSDL uses its common pool of resources only for support functions like personnel, administration, finance, and computer operation.

12.2.3. *Contracting*

Establishing TIN required initial capital investment, regular operating expenditure, and periodic investment for capacity upgrade and modification to accommodate increase in volume and changes in the Income Tax Laws. The Department realized that the normal Government procurement may require lengthy procedure for administrative approval, resulting in delays in implementation. Therefore, the Department developed a financial model wherein the payment is made on the basis of usage of the system. To suit this

Figure 12.1: Information security



business model, the Department also evolved a special Agreement that dened the expected outcome for each module, and risk management policies that included third party audits, SLAs and exit management policies.

12.2.4. *Incubation*

NSDL did not need to be incubated, since it was already operating the depository successfully when the TIN agreement was signed.

12.3. Technology challenges

12.3.1. *Solution architecture*

The modules of TIN as shown in Figure 12.1 are as follows:

1. **OLTAS (Online Tax Accounting System):** A system for all tax collecting banks to consolidate challan level information in the TIN central system
2. **ERACS (Electronic Return Acceptance and Consolidation System):** This consists of an online facility and a network of facilitation centers to accept TDS returns from the deductors' Annual Information Reports from specified agencies.
3. **CPLGS (Central Pan Ledger Generation System):** This is the central system maintained by NSDL where the returns uploaded by filers and challan details uploaded by the banks are consolidated and matched. Subsequently, these systems generate the specified extracts of challan data for ITD and the Office of CGA and the return and PAN ledgers of data for ITD in a manner that will enable processing of returns and provide input for assessment of Income Tax Return. This system also provides a dashboard to various stakeholders for status tracking, monitoring, and control.

12.3.2. *Openness*

TIN has published a plain text ASCII file format for submission of returns by filers and submission of challan data by banks. TIN also provided a free file validation utility that

users could use to verify the correctness of their files before uploading. This approach has proved beneficial to all stakeholders:

1. This open data format helped deductors build functionality in their in-house systems to generate a TDS return on their own.
2. There is no lock-in: of software, or service provider, or even the technology platform for preparation of returns.
3. Many independent software providers built return preparation software in the market, encouraging competition and innovation.
4. Existing financial accounting software packages seamlessly integrated return preparation.
5. Banks also provided similar flexibility for upload of their challan details

12.3.3. *Security*

TIN has put extensive security infrastructure and policies in place to ensure that the security and privacy of data is safeguarded. These are continuously reviewed and upgraded to keep up with challenges in the environment. Periodic audits are conducted by third party auditors, which include security audits.

12.3.4. *Transparency and Privacy*

The Department holds the personal and financial data of the taxpayers in a fiduciary capacity and carries out a sovereign function of the State. Therefore, it needs to have control on strategic assets including the software, hardware and the databases as well as exclusive control over use and dissemination of data. It is recommended, therefore, that TIN should adopt the best practices for transparency and privacy as discussed in this report.

12.4. The way forward

12.4.1. *TIN only a component in IT infrastructure of Income Tax Department*

ITD is a large organisation dealing with tax matters of over 3 crore taxpayers. Its PAN database now exceeds 10 crore records. It annually receives 2.75 crore tax challans, 3 crore returns of income, and 40 lakh TDS returns with information of over 29 crore transactions, besides the AIRs. This is a large and recurring data volume growing every year.

ITD handles its main IT-related functions through a National Data Center (NDC) with its backup sites, connected to offices across the country through a VPN. These have been set up on an outsourced model with three different service providers for Software Solution, Network Service and System Integration. These Service Providers are mainly paid against SLA based contracts, though ITD has also acquired ownership of critical hardware of NDC.

TIN provides ITD's major interface with its customers (taxpayers, TDS Deductors etc) and constituents (Banks, AIR filers etc). Several other taxpayer service functionalities have been set up by ITD using different methodologies and at different times. Thus, hosting and maintenance of its website has been outsourced to two agencies on per transaction basis - a RFP for appointment of a new agency is in progress. Helpdesk support Aayakar Sampark Kendra has been outsourced to another agency. The facility for e-filing of returns of income has been set up departmentally though a RFP for appointment of an agency has been issued recently. A RFP for providing web-enabled services is also in process.

For data processing within the department, the ITD is following multiple approaches. E-filed returns of income and paper returns of Karnataka region are being processed through a Centralised Processing Center (CPC) at Bangalore set up recently on MSP model. The number of these returns has risen to over 60 lakh but the remaining returns of income (2.5 crore) and TDS returns are being processed departmentally on NDC. It is proposed to set up two more CPCs at Pune and Manesar on MSP model. The risk management system is run departmentally on NDC. Data mining of AIR and TDS returns is being done regionally through a customised solution developed departmentally and managed through yet another Service Provider. Computer Forensic labs at Delhi and Mumbai are being run through C-DAC. A Record Management System, Workflow Management System, Judicial Reference System and a Data Warehousing project have been conceived but are yet to be set up. ITD proposes to set up a Special Purpose Vehicle for its IT needs though its exact contours are to be worked out.

It is thus apparent that various IT-related initiatives have been developed or are proposed on different models of implementation for historical reasons. TIN, conceptualised way back in 2003, is only one component of ITD's taxpayer interface. Though it has several features of a NIU with consequent advantages, it is not exactly a NIU in the sense contemplated in this report. The MoU between NSDL and ITD has undergone two renewals and is to now expire in 2011.

The Group notes that the Department is at the crossroads of important strategic decisions as the new Direct Taxes Code is to be operationalised from April 2012 requiring major changes in its application system - which itself was developed in late 1990s, its functional needs in terms of growth of revenues/ number of taxpayers/service standards etc, and required deterrence levels are going to grow significantly over next 5-7 years. The data volumes have grown exponentially. The existing contracts with various service providers are nearing expiry. Although the existing IT related instrumentalities have served the department's needs admirably it may not be advisable to continue with these diverse implementation methodologies.

Considering that its technology needs are large, dynamic, and sensitive from the point of both, security and privacy, the Department clearly needs a dedicated and efficient NIU type organization to set up, manage and run its IT-related infrastructure on long term basis.

12.4.2. *Recommendations*

1. The Group is of the view that time has come for the department to have a fresh and holistic look at its overall IT-related and functional needs over next 5-7 years and to devise a new and comprehensive IT plan keeping in mind the recommendations in foregoing chapters of this report. In its Vision document 2020 the Department has proposed to *meet the challenges of technology by formulating a Strategic Technology Plan*. The Group recommends that this may be done forthwith along with a time bound roadmap for implementation, and all new initiatives should be implemented only in accordance with this Plan.
2. As part of the Strategic Technology Plan ITD must clearly identify IT-related activities and services that it can actively outsource to a NIU and those which it must necessarily handle departmentally. Ideally ITD should directly handle only matters involving policy making, quasi-judicial decision making, exception handling, risk management and enforcement functions. The IT systems required to assist and enable its functionaries in discharge of these should be set up, managed, and run by a NIU.
3. There is a strong case for a separate well-capitalised and professionally run NIU to handle the IT-related needs of ITD. This should be set up on priority

and in accordance with the recommendations in the foregoing chapters. While ITD should retain Board level strategic control, the NIU should have financial autonomy and operational freedom and its affairs should be managed by an eclectic mix of IT experts, management professionals and domain experts.

4. Such a NIU would necessarily need services of a few departmental officers as domain experts at different levels to enable it to discharge its mandate. It should therefore be possible for suitable departmental officers to be deputed to the NIU for a defined period while retaining lien on their cadre posts. The relevant Rules may be accordingly modified to enable deputation/secondment of a few officers to the proposed NIU.
5. Action points 4 and 5 of ITD's Vision 2020 document require it to *resolve multiplicity of platforms in favour of uniform holistic rule based application matrix* and to *integrate all the elements of tax collection process through technology with information seamlessly flowing to the users for informed decision making*. This Group entirely endorses these and recommends that these should be implemented at the earliest.
6. The Ministry of Finance should develop the next generation Risk Information Network to enhance the effectiveness and impact of tax collection using functionalities such as comprehensive taxpayer profiling, trend analysis, pattern recognition, and data mining of the information gathered in ITD, GST, and Customs systems.
7. Simultaneously the Department needs to restructure and reorganise the Directorate of Systems and re-define its role as the department's single point interface with the NIU so as to take full advantage of the NIU model. As part of this exercise it may also re-determine the strength of its technical cadres and restructure the same.

13

Expenditure Information Network

13.1. Introduction

In the mid 1980's, the then Prime Minister Shri Rajiv Gandhi had estimated that of every rupee spent on development only 15 paise reached the poor. Apart from administrative inefficiencies, poor targeting, and high implementation costs, there is often a big hiatus between the release of funds by the GoI and actual expenditures on the ground.

As a 2007 Planning Commission Working Paper [1] pointed out:

> The connection between release of funds by the Central Government and actual expenditures for physical inputs by the implementing agencies is currently, very obscure.

The office of the Controller General of Accounts is already implementing the Central Plan Scheme Monitoring System (CPSMS), which aims to establish a suitable on-line Management Information System and Decision Support System for the Plan Schemes of the GOI. A lot of work has been done in this area. However, moving forward, the vision of the EIN as articulated in this report should be the next priority of the Government.

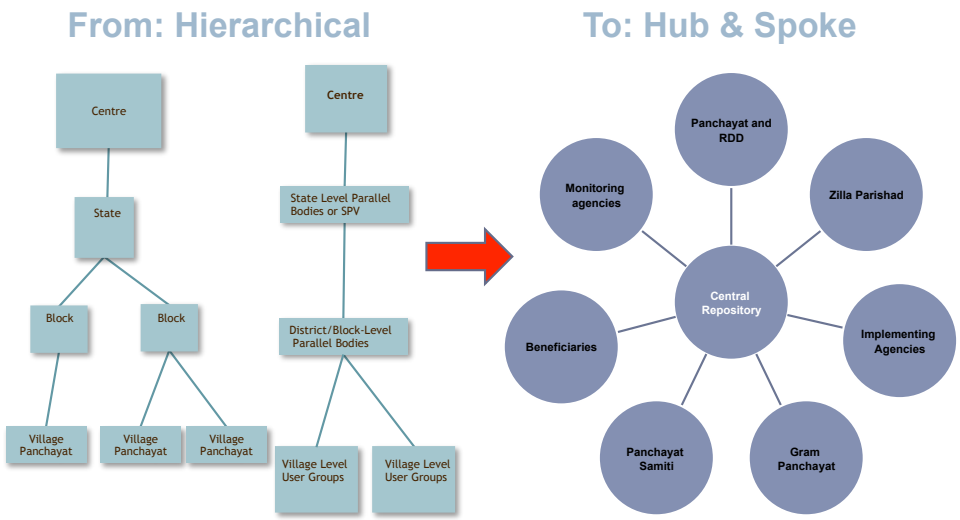
13.1.1. *Challenges with expenditure tracking today*

Today, the GoI's budget documents do not report on actual expenditures at the level of implementation. Data on expenditures can be found in the annual audited accounts of the Government but these have nearly a two year time lag. Disaggregated expenditure data is often only available up to the district level and not below. This makes it difficult to perform data analysis for program evaluation. A well functioning system that makes this information available in real-time will greatly improve transparency, policy-making, and eventually lead to more effective governance.

The existing system of transfer and monitoring of funds has some limitations. Today, measurement of plan schemes and programs is largely on the basis of outlays rather than outcomes. Government follows hierarchical and multiple patterns for allocation and release of funds to the implementing agencies and beneficiaries. It is difficult to

[1] Virmani Arvind (2007), Planning for Results, Planning Commission Working Paper No. 1/207-PC.

Figure 13.1: EIN: From hierarchical to hub-and-spoke reporting



track the flow of funds to actual beneficiaries, and equally difficult to evaluate the performance of agencies based on spending and project implementation.

Apparently, there is significant float of funds in the system, the cost of which due to inefficient use is eventually borne by the taxpayer.

13.1.2. *Setting up an Expenditure Information Network*

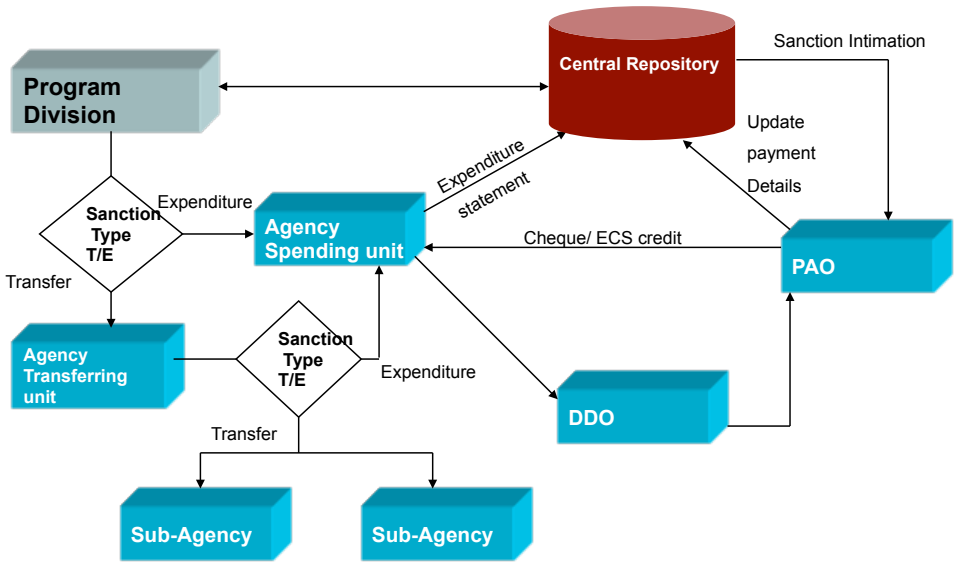
There is a need for effective monitoring, evaluation and accounting system for the funds that are disbursed by the Central Government to State Governments, district level agencies and other implementing agencies as Plan Expenditure[2] .

The establishment of an integrated Expenditure Information Network is a step in this direction, and can help achieve the following objectives:

1. Monitoring scheme-wise release of funds and outcomes
2. Helping in budgeting, planning and decision making based on the evaluation of all plan schemes
3. Maintaining time-series information related to each implementing agency, which will enable in evaluating performance
4. Ensuring disbursal of funds to intended beneficiaries
5. Ensuring timely disbursal of funds
6. Reducing float of funds within the system
7. Up-to-date and near real-time information on utilization of funds
8. Monitoring of outcomes up to the last mile
9. Transparency in disbursal and utilization of funds by making information available in public domain by way of a transparency portal

[2]Finance Minister's Budget speech in 2008–09 (Paragraph 115): http://indiabudget.nic.in/ub2008-09/bs/speecha.htm; Economic Survey 2007–08: http://indiabudget.nic.in/es2007-08/esmain.htm

Figure 13.2: EIN solution architecture: Information flow



13.2. Public policy challenges

The Group recommends that the NIU framework as described in Chapter 1 be followed. Aspects such as allocation of tasks between the Government and the NIU, appointment of a dedicated Mission Leader and a dedicated Mission Execution Team (Chapter 2) may be along the lines of the recommendations contained in this report.

Some of the challenges anticipated in the implementation of EIN are similar to those being faced in the context of GST. The relationship between the Government and the NIU may be defined by an Agreement as described in Chapter 3. EIN may be incubated as per the recommendations in Chapter 4 of this report. Learnings from the experience of setting up GSTN should be adopted in setting up the NIU for the implementation of EIN.

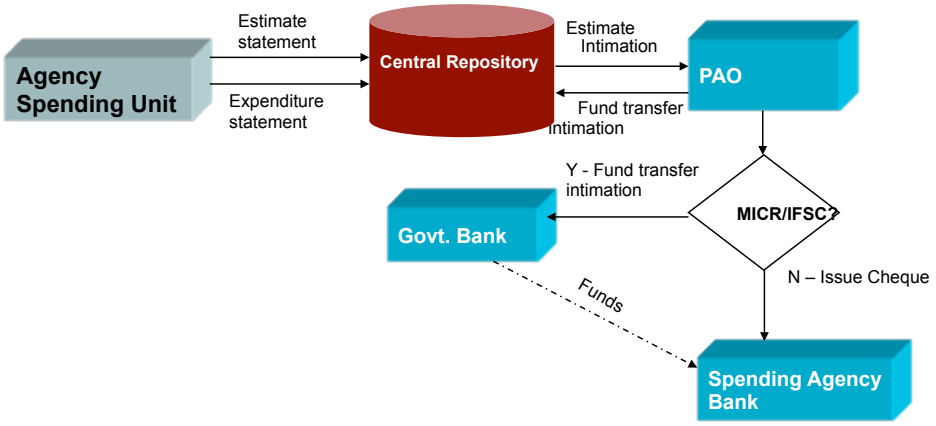
The EIN solution should provide for tracking of expenditure at Central, State, and Local levels. Therefore, the solution should ensure balance between standardisation of features and autonomy of States as provided in Chapter 5. Appropriate incentives should also be devised for full participation at all levels of Government.

13.3. Technology challenges

The solution architecture for EIN should have the following features:

1. The hierarchical functions of allocation, authorization, disbursement, and utilization may continue as at present, but the reporting mechanism should be based on a hub and spoke model as shown in Figure 13.1. This arrangement will help in correct and prompt capturing of expenditure information.
2. The Central Expenditure Repository (CER) is a key ingredient of the design of the EIN. EIN will handle the information flow through this repository (Figure 13.2).
3. The flow of funds will be managed through the banking system (Figure 13.3). Banks can make an electronic transfer in case the account is available in a CBS

Figure 13.3: EIN solution architecture: funds flow



branch, or issue a cheque. Banks would then report the details of disbursals to EIN for reconciliation purposes.

4. EIN will track all authorizations and forward electronic instructions to banks, so that funds move only against actual expenditure to service providers.
5. Planning Commission, Ministries, Departments, and Program Divisions can be linked to CER and should be able to monitor the outcomes, utilization and fund status through near real-time availability of information about all entities and programs.
6. Pay And Accounts Office (PAO) should be able to view the payment authorizations marked in EIN and release funds to spending agencies.
7. Program Divisions at various ministries should be able to set first leg of fund flow transaction (allocation of funds to parent agency). Funds disbursed to States should be marked as *Transfer* and not *Expenditure* if the funds are meant for further distribution to implementing agencies.
8. All the agencies such as State bodies, district bodies, village panchayats, block level bodies, and beneficiaries should have access to EIN with appropriate access controls. These agencies can view the funds sanctioned for them and also update the status of utilization of funds by them.
9. For greater transparency, citizens should also have access to a transparency portal and information from the ground can be crowd-sourced.
10. All financial information made public through a transparency portal should be machine-readable and format-neutral.
11. EIN should enable easy download of data and reports to facilitate the evaluation of the impact of public expenditure.

13.4. The way forward

The EIN project is similar to the GST project in many ways. Some of the processes touch more agencies and involve more steps. The Group recommends that the measures suggested for GST (Section 11.4) may be suitably adapted for the implementation of EIN.

14

National Treasury Management Agency

14.1. Introduction

In the 2007–08 Budget speech, the Honourable Minister of Finance announced that a Debt Management Office would be set up[1]. This drew on the recommendations of the HPEC Report on Mumbai: An International Financial Centre[2]. In light of these developments, the Ministry of Finance formed an Internal Working Group to analyse how best to move forward on establishing a Debt Management Office. The report of the Internal Working Group on Debt Management — Establishing a National Treasury Management Agency (WG) [3] — lays down a framework on setting up the NTMA. The NTMA will manage debt for the Centre and States, with the overarching objectives of meeting their financing needs, while minimising borrowing costs within acceptable levels of risk.

14.2. Public policy challenges

The Group recommends following the NIU framework as described in Chapter 1 for NTMA. As recommended in the Report of the Internal Working Group on Debt Management, NTMA should have a dedicated team to manage its operations. The Group recommends that the HR structure for Government teams (consisting of a Mission Leader and Mission Execution Team) as recommended in Chapter 2 should be adopted for NTMA.

14.3. Technology challenges

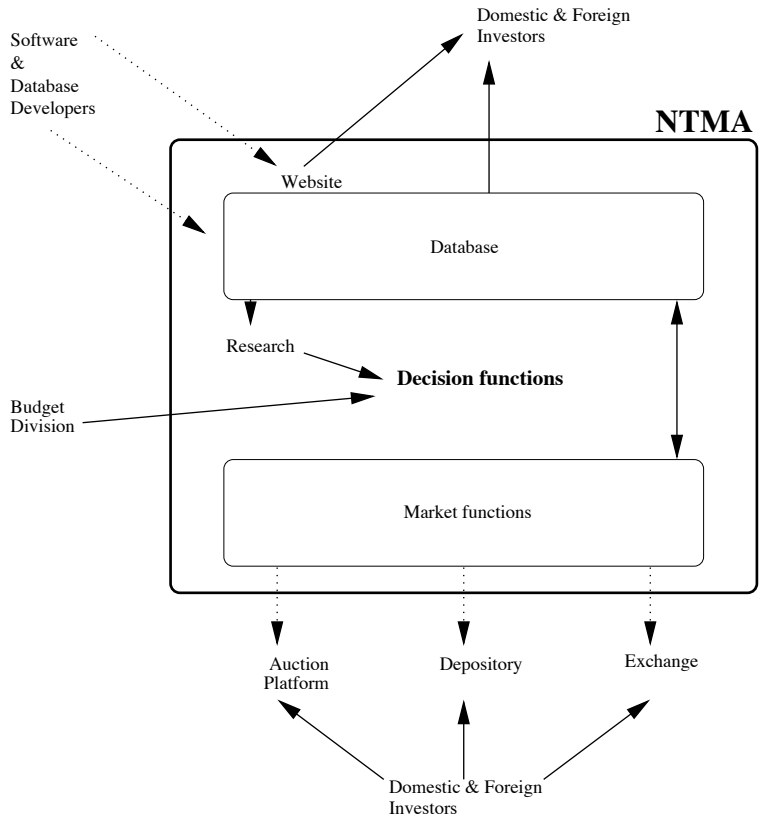
The WG has recommended the solution architecture for NTMA, which is shown in Figure 14.1. The Group commends this approach.

[1]Finance Minister's Budget speech in 2007–08: http://indiabudget.nic.in/ub2007-08/bs/speecha.htm

[2]Report of the High Powered Expert Committee on Making Mumbai an International Financial Centre: http://finmin.nic.in/the_ministry/dept_eco_affairs/capital_market_div/mifc/fullreport/execsummary.pdf

[3]Establishing a National Treasury Management Agency: http://finmin.nic.in/reports/Report_Internal_Working_Group_on_Debt_Management.pdf

Figure 14.1: NTMA solution architecture



The WG has a strong focus on openness, transparency, and developing a strong research capability. The Group recommends that NTMA should also adopt the best practices for solution architecture, openness, transparency, security, and privacy as described in this report.

14.4. The way forward

The WG provides detailed steps for incubation, which span legal issues, setting up of IT systems, and change management for transferring the functions from RBI to NTMA. The Group recommends that the incubation framework, and creation of the platform described in the WG report may be adopted.

15

New Pension System

15.1. Introduction

In 2004, the Government of India introduced a new defined contribution pension scheme known as the New Pension System (NPS), replacing the existing system of defined benefit pensions. The NPS was envisioned to provide financial security to its subscribers after retirement while ensuring that the costs of pensions account administration, fund management charges and other expenses are low.

The Government established the Pension Fund Regulatory and Development Authority (PFRDA), as the apex body to regulate and develop the pension sector in India, to provide old age income security for all individuals, including those in the unorganised sector.

PFRDA has put in place an institutional framework with a set of Intermediaries who have experience in their respective areas of operations such as record keeping, fund transfers, fund management, custodial services etc. The relationships between various stakeholders are shown in Figure 15.1.

15.2. Public policy challenges

15.2.1. *Placement of tasks: NSDL as the MSP*

PFRDA is responsible for designing the institutional architecture, framing the policies for functioning of NPS, selecting and regulating various intermediaries for record keeping, fund management etc. The record keeping function is performed by NSDL, who runs the Central Record keeping Agency (CRA). The current placement of tasks is similar to that of an NIU as described in Chapter 1.

15.2.2. *Human resources*

The PFRDA provides for a Chairperson and not more than five members, of whom at least three shall be whole-time members, to be appointed by the Central Government.

The other officials include two Executive Directors who have their team of officers drawn from various Government departments. PFRDA is in the process of enhancing its

team by infusing talent from outside. The Group recommends infusing the team at PFRDA with market professionals.

For each of the major intermediaries like CRA, Pension Fund Managers, etc., PFRDA has prescribed establishment of exclusive business units to perform the functions related to NPS. Each of these intermediaries is regulated by PFRDA and is assisted by process owners for each key process.

15.2.3. *Contracting*

PFRDA engaged external consultants to assist in developing the RFP for the solution architecture, system specifications and contracts. The contracts with intermediaries prescribe the roles, responsibilities, charge structure, service level agreement, penalty structures, exit management mechanisms,etc.

15.2.4. *Incubation*

Various intermediaries such as the CRA, Fund Managers etc were selected on the basis of an open and transparent competitive bidding process managed by PFRDA. Subsequently, PFRDA has been actively monitoring the establishment of each of these agencies.

The various stakeholders in NPS are as follows:

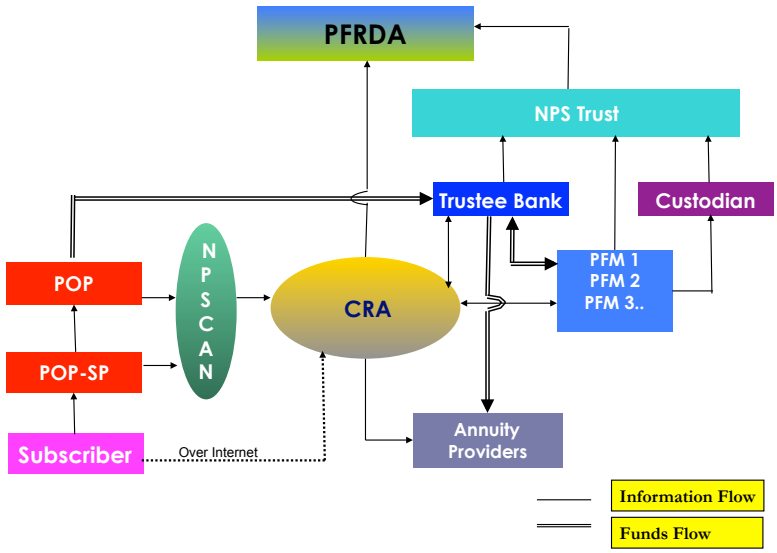
1. **CRA:** In the NPS architecture, the CRA forms the foundation on which the long-term success and stability of NPS rests. CRA maintains complete records of all clients with respect to their subscription, scheme choice, units allocation, scanned copies of their documents etc.
2. **Fund Managers:** They handle the investment of the funds collected within the contours of the prescribed guidelines.
3. **Custodian:** Custodian handles the back office functions for the fund managers.
4. **Annuity Providers:** They will provide monthly pay-outs to individuals after retirement based on the accumulated pension wealth.
5. **Trustee Bank:** The Trustee Bank consolidates the funds uploaded by the subscribers (directly or through intermediaries) and forwards them to the fund managers, based on the input consolidated by CRA.
6. **Entities for servicing the subscribers:** In case of Government employees, the accounts officers (Pay and Accounts Officer / CDDO for Central ministries or treasury officers for State Government) handle the consolidation of subscriber contribution , transfer of the funds to the trustee bank, and uploading the subscriber contribution files to CRA. In case of subscribers in the unorganised sector, the client servicing is handled by Points of Presence(PoPs) registered by PFRDA.

15.2.5. *Multiple levels of Government*

Central Government has adopted the basic architecture designed by PFRDA for all Central Government departments, with a few exceptions. State Governments have the freedom to adopt the NPS architecture and the associated institutional infrastructure or to establish their own mechanism and infrastructure, or to continue with their current pension system.

All States joining the NPS are required to sign separate agreements with intermediaries such as the CRA. However, PFRDA strives to ensure that the solution and contract remains standard for all entities that participate in NPS.

Figure 15.1: NPS solution architecture



15.3. Technology challenges

15.3.1. *Solution architecture*

The detailed solution architecture for NPS is shown in Figure 15.1. The salient features of the NPS are:

1. NPS has already been operationalised for new Central Government employees through a notification with effect from January 1, 2004.
2. Every NPS subscriber has an individual pension account with a unique Personal Retirement Account Number (PRAN), which will be portable across jobs and locations. NPS will also offer seamless transfer of accumulations in case of change of employment and/or location.
3. NPS offers a basket of investment choices and pension fund managers. The subscriber can choose any fund manager and scheme and has the option of switching schemes and fund managers
4. Provides services for opening of Individual Retirement Account (IRA), and issuing PRAN Card, I-PIN, and T-PIN to account holders, through the CRA.
5. Offers Tier-I (pension, non-withdrawable) and Tier-II (withdrawable) accounts.
6. Implementation framework allows a combination of retailers, pension funds and multiple recordkeepers.
7. Uses existing network of bank branches and post offices to collect contributions and deliver services to customers across the country.

Though the CRA system was developed on the basis of a standard specification evolved by PFRDA, the operationalisation of CRA services to Central, State and all India segments threw up a number of challenges in terms of the way data is maintained by accounting offices at various ministries, issues related to discipline in handling pension contribution deductions, and quality of the data maintained by them.

PFRDA and CRA have been making continuous refinements to the basic solution and business processes to meet the varying requirements on the basis of the feedback

received from the users. Some examples of these enhancements and improvements include:

1. Facilitates easy adoption through registration of nodal offices and subscribers and enabling them to commence the subscriber contribution quickly.
2. Multiple interface models to accommodate the requirements of various State Governments and Central Autonomous Bodies (CAB) who have joined NPS.
3. Utilities for contribution processing to accommodate varying requirements relating to fund transfer and interfacing models across organizations.
4. Enhanced features to help the various oversight bodies and to satisfy the special requirements of various entities like Points of Presence (POP), States etc.
5. Exception handling in case of mismatch in Subscriber Contribution File and funds transfer for streamlining process compliance by nodal offices.
6. System stabilization and exception handling in case of poor data quality.
7. Management reports and dashboards
8. Grievance management to analyse the grievance patterns and bring about systemic improvements in CRA systems and processes
9. SMS alerts to IRA compliant subscribers

15.4. The way forward

1. In order for a well-ordered and mature pension business to develop in the country, there is a need for:
   (a) All pension and provident fund streams to converge in the medium term;
   (b) Costs to go down dramatically due to competition and economies of scale; and
   (c) Rule-based regulations need to give way to principles / risk-based supervision.
2. An enabling legal framework that provides the necessary impetus for NPS should be provided.
3. The tax treatment of the NPS also needs to be rationalized to provide for, at least equal treatment with other retirement products and providers.
4. There is an imminent need to create a certain level of awareness amongst the NPS subscribers that will eventually empower them to make well informed investment choices to protect and further their own interests.
5. As the broader mandate of the PFRDA is to regulate the pension sector in the country, this may eventually necessitate the separation of the NPS administration, including marketing and distribution strategies, from the PFRDA.

Recommendations

1. NPS needs to create a daily MIS with facts about number of subscribers, assets under management, the breakdown of number of subscribers and assets under management under various heads of Government, the number of switches made by customers from one fund manager to another, the returns of the various schemes of various pension fund managers, and summary statistics about the returns obtained by NPS members. The daily release of this information base is essential for policy analysis and the creation of self-correcting forces.

2. NPS should to create an audit mechanism whereby every year, for randomly chosen customers in a statistically meaningful way, a comprehensive review is undertaken about correctness of data, about whether contributions came in on time, and about whether each member was notified about every contribution. The results of this audit should be released into the public domain. This will yield a regular check upon the quality of performance of NPS.
3. There is a need to avoid splitting the functionality of NPS across multiple variants of the same product, since the existence of variants reduce portability for customers and increase cost.
4. While significant strides in IT implementation have been undertaken in the NPS, there is a need to further leverage recent technological innovations in e-Governance, banking, and financial networks to develop greater efficient mechanisms that leverage use of IT in an end-to-end manner – from the post office interacting with the customer to the CRA to the fund manager and annuity providers.
5. More specifically, initiatives may be taken in the following areas to develop a comprehensive integrated pension administration system:

    (a) Enabling linkages with HR and payroll systems of the Central and State Governments to obtain subscriber contribution details, among other things.

    (b) Revamping and automating all pension administration processes.

    (c) Re-engineering in the context of the user departments, especially in areas related to Government accounting formations

    (d) Providing process linking between Government accounting systems and the pensions administration system

    (e) The implementation of these initiatives should be accompanied by extensive skill enhancements, learning and change management efforts, in conjunction with nationwide public awareness campaigns.

6. As the Aadhaar implementation becomes ubiquitous across the country, there is a need to establish the platform for linking Aadhaar with the PRAN number, which can enable Aadhaar-linked KYC for pension scheme enrollment. In this aspect, the NPS should also explore opportunities for future integration with the identification and authentications systems of the Unique Identification Authority of India (UIDAI).

Part IV

Summary of recommendations

16

Recommendations for public policy challenges

16.1. The appropriate placement of tasks

1. For complex projects that depend on mission-critical IT systems, National Information Utilities (NIU) working in the spirit of partnership with Government may be put in place to handle all aspects of IT systems. They would participate in high-level design, specification of requirements, proof-of-concept studies, while strategic control would remain with Government. (1.1)
2. NIUs would be set up as private companies with a public purpose: profit-making, but not profit maximizing. The NIUs should be financially independent and empowered to take quick and efficient business decisions pertaining to attracting and retaining talent, procurement, rapid response to business exigencies, adopting new technologies etc. They should be able to get funding independently and have a self-sustaining financial model. (1.3.1)
3. Strategic control can be achieved by having a strong dedicated team within Government inter alia to drive policies, design a suitable solution architecture, supervise execution, frame appropriate contracts, adopt outcome based pricing, evolve strict service level agreements (SLA), and conduct independent audits. (1.3.2)
4. An NIU should be structured as a company with limited liability and be subject to sound corporate governance norms, such as those required for listed companies though the company may not be listed. The board composition, accountability, and transparency norms for NIUs should be the same as prescribed for listed companies. (1.3.3)
5. Other characteristics of an NIU should, inter alia, be:
   (a) ownership share of the Government in it should be at least 26%;
   (b) total private ownership within it should be at least 51%;
   (c) no single private entity should own more than 25% of the shares in an NIU;
   (d) institutions that have a direct conflict of interest (e.g. IT companies) should not be permitted to be shareholders;

(e) an NIU should not go for an initial public offering or list itself on public exchanges;

(f) an NIU should be dispersed-shareholding corporations with a professional management team;

(g) an NIU should preferably have a net worth of Rs.300 crore. (1.4)

6. NIUs, though set up initially as natural monopolies, would be obliged to provide access to a competing NIU, when one emerges. (1.4.1)
7. For effective functioning, an NIU should be, self-financing, making reasonable profits, and having sufficient net worth' to meet exigencies. It should maintain high professional standards and competitive practices, utmost transparency in its operations, be willing to invest in technology for increasing efficiency, reach and economies of scale. (1.4.1)
8. Government-NIU relationship may be defined by an Agreement, which covers allocation of tasks and responsibilities between the Government and the NIU, financials, and SLAs. (1.5)
9. In the early phases of a project, during incubation, both, the Government and the NIU should have teams that are dedicated to the project, which will facilitate smooth decision making. (1.5)
10. Business change is the driving force, and technology is an enabler. Therefore, a Mission Strategy Document for the project that inter alia details the functions, and capabilities of the IT System which would assist in bringing about the desired business change, should be prepared. (1.5)
11. While the Department should recognize the capabilities and limitations of the technology solution, the NIU should perceive its responsibility as extending beyond merely meeting a technical or legal requirement under the Agreement with Government. (1.5)

16.2. Human resource policies

1. Strong support from the top management within Government, leadership at the level of project implementation, and ownership and commitment at various operational levels are necessary concomitants of success of any project. The concerned Department should put in place a high level body that will review the progress of the project during its implementation and later evaluate the realization of benefits and objectives on a periodic basis. (2.1)
2. Every project should have a dedicated Mission Leader within the Government Department, of the rank of Joint or Additional Secretary, fully responsible for the project. This person should possess necessary technical and managerial skills. This post should be open to all eligible officers of the Government. The Mission Leader should have the freedom to choose the Mission Execution Team from within or outside the Government. (2.3.1)
3. The Mission Execution Team should be manned by personnel, who possess a diverse set of skills including intimate familiarity with the Government processes, specialisation in verticals such as technology, outreach, law, as well as the ability to manage a large decentralized organization, among others. This team, including the Mission Leader, should have adequate tenure (at least 5 years) for purposes of continuity, so that institutional memory can be created and retained. (2.3.2)

4. Professionals may be hired into the Team by posting suitable officers to the project from the same cadre; inducting officers on deputation from other departments at suitable compensation under the Central Staffing Scheme; infusion of talent from the private sector by way of lateral entry; hiring professional resources on contract basis; by appointing consultants at market rates on contractual basis; recruiting sabbaticals from industry, who continue to be employed by the parent organization; recruiting volunteers who come from various walks of life through a well-defined volunteer selection process; and recruiting students from various colleges and universities as interns through a well-defined internship program. (2.3.3)
5. Just as the Government team will have business specialists, and experts from other domains, so should the NIU have a management team with the right domain knowledge, and other essential expertise in areas such as technology, law, and outreach. The NIU should also take on its staff, professionals from the Department, who have the requisite business domain knowledge, so that the IT systems they develop and implement is backed by people with relevant domain experience. (2.4)
6. Government should set up a database of all IT projects implemented in the public sector, containing comprehensive details of the individual projects and the key personnel associated with the project. Centres of Expertise within the country may be identified for providing assistance by way of project consultancy and advanced training in the field of IT management. (2.5)
7. With a view to building capacity within the Departments embarking on large, complex projects with mission-critical IT systems, the training curriculum for the existing workforce of various services should include training on the technical aspects of IT systems, project management and evaluation, procurement management, governance issues, and change management. Mid-career programs should also be designed in such a way that senior officers are not only able to provide the required leadership but also coach and mentor junior managers. In-service personnel, who already possess technical knowledge should be trained in the latest technologies and in fields in which they like to specialize. (2.6)
8. As a measure to retain in-service staff deployed in IT functions they should be provided with IT professional allowance on the lines of the training allowance at the rate of 30% of their remuneration. (2.6)
9. The Performance Linked Increment Scheme as suggested by the Sixth Pay Commission for Central Government employees, should be implemented along with performance linked training programs in special skills. (2.6)
10. A scheme of non-monetary incentives such as public acknowledgement of their contributions, certificates of outstanding performance etc. should be instituted with a view to motivating both in-service officers and contracted personnel. (2.6)
11. Full opportunity should be provided for every individual to equip himself for higher levels of responsibility through individual and group assignment and training programs to ensure that his/her needs are satisfied. (2.6)
12. For creating a conducive work environment, end users should be provided appropriate training and support and encouraged to make their own contribution to the success and continuous improvement of the project outcomes. (2.7)
13. The method of performance appraisal has to be reconsidered, by redefining the purpose and principles, conducting a job analysis, obtaining employee feedback, reviewing standards of objectivity, conducting training for both managers and employees and reviewing/evaluating the results of the system. Greater objectivity

and according appropriate weight to the overall contribution of the individual has to be given due consideration. Merit should be given primacy over seniority within a given band of eligible appointees. Adoption of performance management techniques would be particularly relevant for appraising the performance of in-service officers entrusted with the task of implementation of mission-critical projects. (2.8)

16.3. Contracting

1. In general, the relationship between the supplier and the Government should ensure that:

   (a) the solutions proposed by the supplier focus on and meet the business needs spelt out by the Department owning the project and not just the technical, operational, or legal requirements;

   (b) through the lifecycle of the project the supplier should produce realistic plans, including timeframes, resources, technology, mode of delivery and financials, and align the same with the business needs;

   (c) the supplier should as far as possible maintains continuity in employing trained Personnel;

   (d) both should share in a timely manner all information about technical, financial, and personnel problems, set up a mechanism for co-operation and dialogue;

   (e) both should agree and document change control processes, address risk factors and avoid informal changes.

   (f) both should recognize that estimates of price, timeframes should be realistic and achievable. (3.1)

2. The Agreement between an NIU and the Government should clearly set out all aspects relating to the scope of work, activities to be undertaken by NIU, obligations of the Government and NIU, the financial arrangement, Service Level Agreement, and business continuity plan upon exit. (3.2)

16.4. From startup to going concern

1. While a project itself may be housed within one of various available institutional frameworks, an NIU that serves the project should necessarily follow the structure as described in Chapter 1. In the case that a new NIU is being created to support a particular project, it can be incubated within an existing NIU. Subsequently, when the project achieves some level of maturity, the project team and project assets (tangible and intangible) can be spun off. (4.3)
2. The project should prepare a Mission Strategy Document that describes the project, the stakeholders, the broad legal framework, the solution architecture, the nature of the platform, role of the ecosystem, and potential pricing. (4.4)
3. Best teams should be put in place within Government and within the NIU. (4.5)
4. Consultations with stakeholders e.g.multiple levels of Government, other Government Departments, NIU, Banking system (if funds are involved), service providers, and customers and end-users. (4.6)

5. A legal framework, with enabling policies may be necessary for a project to go live. This may require passing a Bill, modifying subordinate regulation in centre and State Acts, or in some cases, a constitutional amendment. A strong legal team working with all stakeholders is a must for every project. (4.7)
6. The project should be rolled out as soon as possible, and iterated rapidly, rather than waiting to roll out a perfect system. (4.8)
7. The Government's role is to set policy, co-ordinate with other Departments, and provide strategic direction, whereas the NIU focuses on execution and implementation.In the early stage, the Government agency / Department works alongside the NIU and as the system starts falling into place, the role of Government changes to:

   (a) Conducting proof-of-concept studies

   (b) Giving feedback on mis-features, bugs and additional specifications, and

   (c) Setting up the institutional capability for scaling. (4.9)

8. Once the rollout is completed, the Government's role shifts largely to that of a customer. It should compute metrics of performance of the system in all respects such as performance, cost, accuracy, and release these into the public domain. Quarterly reviews of the performance of the system should be undertaken. (4.9)

16.5. Multiple levels of Government

1. IT projects that span multiple levels of Governments may be classified into two types:

   (a) Projects such as GST, NTMA, and EIN where the NIU aids the core function, or aids carrying out a sovereign function of multiple levels of Government.

   (b) Projects such as NPS, where the core function is carried out by a Central agency, but co-operation among Government agencies is required for the purposes of uniformity, standardization, interoperability to maintain levels of service and drive economies of scale. (5.2)

2. A critical aspect of the success of such IT projects that the solution must be incentive compatible across stakeholders. Common functions should be included in a single application shared by all stakeholders. Such a single application, while respecting the constitutional autonomy of all Governments involved, may be deployed in a decentralized environment, but its development must necessarily be centralized. (5.3)
3. The two activities, consensus building and solution design need not necessarily be sequential. The basic design and the details of the implementation can be put in place while policy details are being debated. (5.4)
4. Common minimum functionality can be built into a Common Portal, in such a way that its basic functionality can be enhanced by local customizations such as look and feel, local languages, and local policies, to mention a few. Such a design allows for low cost, scale, interoperability, speed, simplicity, a uniform customer experience, and portability of service. (5.4)
5. The following steps could be adopted for projects that span multiple levels of Government:

   (a) identification of all stakeholders;

(b) formation of an Empowered Committee of representatives drawn from every stakeholder;

(c) appointment for all decision making, a smaller Empowered Group;

(d) creation of an NIU for the execution of the project. (5.5)

6. The project should release a Mission Strategy Document that guides the implementation. The process laid out for incubation of Government projects and NIUs would foster a coalition for change early on in the life cycle of a project. (5.6)

17

Recommendations for technology challenges

17.1. Solution architecture

1. At the outset of a project, the long term IT strategy should be conceived and published as part of the Mission Strategy Document. A functional system diagram should be created that captures the following at a conceptual level:
   (a) Role of multiple levels of Government
   (b) Key business processes and workflows (information flow, funds flow, etc.)
   (c) Integration with various stakeholders (6.2.1)
2. A structured change management process should be put in place, so that the process is incremental. A principle of least surprise to the user, so that minimal change in user behaviour is required, is a good principle to guide the change management process. (6.2.2)
3. Changes in policy should be accompanied by the corresponding changes in IT systems; the two should go hand-in-hand. (6.2.3)
4. Clean data should be ensured by standardisation of processes, matching and verifying information in workflows, simple and well defined open data formats, electronic payments and processing, instant feedback to customers, incentives for compliance, and penalisation for non-compliance. It is through incentives that data quality can be managed, rather than micromanagement of stakeholders. (6.2.4)
5. Interoperability among multiple service providers is essential to foster competition in the long run. This can only be achieved if interoperability is built into the system architecture from the outset. (6.2.5)
6. The solution architecture should be designed as a Service Oriented Architecture that allows stakeholders to integrate with the IT platform of the project. (6.2.6)
7. conceptualisation of a platform approach to service delivery entails that at the front-end, the data entry and retrieval architecture must be real-time and ubiquitous. In order to enable this, data connectivity at the front-end is

critical. The Government should make it a top priority to provide connectivity ubiquitously. Implementation of Aadhaar for proof of identity and address for telecom connections across all stakeholders should be rolled out for greater telecom inclusion. (6.3.1)

8. In order to minimise errors in identifying individuals (as beneficiaries under various schemes) and firms and ensure foolproof ways for transactions to be authenticated,

   (a) Efforts should be dovetailed with the Aadhaar initiative for unique identification of individuals

   (b) PAN numbers should be used for unique identification of institutions. (6.3.2)

9. Access to bank accounts should be universal, so that Government payments can be made seamlessly. Implementation of Aadhaar for proof of identity and address for opening bank accounts across all stakeholders should be rolled out for greater financial inclusion. (6.3.2)
10. An Aadhaar Payments Bridge should be designed by all stakeholders to ensure seamless delivery of Government payments to beneficiaries. (6.3.2)
11. The Government should closely work with all stakeholders to define a uniform banking interface for Government, so that inter-Government payments may be tightly integrated with internal processes within Government. (6.3.2)

17.2. Openness

1. The use of open standards in the design and implementation of open standards is highly desirable in IT systems. Multiple vendors provide competing solutions that can be used interchangeably with open standards. (7.2)
2. All projects should be active producers and consumers of open data. (7.3)
3. Open source software should be adopted in projects as prudent. (7.4)
4. The Government in partnership with concerned stakeholders should set up an open source foundation to host open source software released by Government projects. (7.4.1)

17.3. Information security

1. As use of mission-critical IT systems becomes widespread within Government, the growing connectivity between these information systems, the Internet and other infrastructure, create opportunities for increasingly sophisticated attacks on such systems. Such attacks may be made by individuals, non-state players, as well as by hostile Nations. It is therefore essential to ensure that any disruptions of critical Government information systems are contained and managed effectively to minimize their impact. (8.1)
2. The security team for important projects must be best in class, and the security solutions must always be cutting edge at all times. (8.1)
3. A Chief Information Security Officer (CISO) should be appointed who is empowered and fully responsible for all aspects of information security: technology, processes, and people. (8.2)

4. Security must be part of the ethos of the organization, and can only be achieved when the entire organization (right from senior management to field personnel) is geared for it. This requires training and awareness on basic facts about information security (strong passwords, how systems are hacked, denial-of-service attacks, social engineering, de-mystifying jargon etc.) all levels. (8.2)
5. Various international standards and best practices can be customized to define a comprehensive certification framework (8.2.1)
6. Technology reviews, process reviews and third party reviews should be conducted on an ongoing basis. (8.2.2)
7. Security should be an integral of the solution architecture, and not an afterthought. As part of the security architecture, the following ideas should be considered: identity, access and entitlement management, host access management, data encryption, data hashing, data classification and data loss prevention, transaction auditing, and interaction security. (8.3)
8. Protections must be put in place to address the threat to security from insiders. (8.4)
9. The security teams of individual projects should integrate with existing agencies set up by the Government such as CERT-In1, and with other frameworks that evolve over time. (8.6)

17.4. Accountability, transparency, and self-corrective forces

1. The architecture of an IT project must be designed keeping a transparency portal in mind. A large IT project produces large volumes of data daily. If a transparency portal is designed as an afterthought, the end result may be lack-lustre. (9.3)
2. The same software architecture for data warehousing, data mining and business intelligence required within an IT project for policy support and analysis can also support the operations required for a transparency portal. (9.3)
3. All the data should be made available in simple, well-defined, machine-readable formats. (9.3)
4. A transparency portal leads to monitoring and feedback at various levels: within the service provider, within Government, and by citizens at large. It is an essential part of self-corrective forces that lead to greater accountability and transparency. (9.4)
5. contact centre closes the feedback loop of self-corrective forces. It establishes multiple channels of communication with all stakeholders, including end-users, for purposes of gathering information and reporting grievances. It should provide service in multiple languages, through multiple channels, and be integrated with the solution architecture of the project. (9.5)
6. Enabling citizens and beneficiaries of public schemes to directly provide feedback using web and mobile phone-based platforms is a powerful way of involving citizens in improving public accountability. It unlocks the potential of collective wisdom. (9.6)

17.5. Protection of the individual

1. The solution architecture of a project should be designed for data protection and privacy from the ground up. (10.2)

2. The privacy framework for a project should be defined early on, which translates the legislation on privacy into implementable rules for IT systems. (10.2)
3. The design of the solution architecture should ensure that any Personal Identifiable Information (PII) is stored safely, and access is carefully monitored. Stringent penalties must be in place to address the issue of unauthorized access of personal data by outside agencies as well as by personnel within the organization. Strict protocols and processes must be in place to detect such access in order that they are dealt with swiftly and in a deterrent manner. This is not only desirable from a privacy perspective, but also from a security perspective. (10.2.1)
4. Anonymization of data is an important aspect of privacy. Data should be carefully anonymized when released publicly, or when shared with other organizations that do not require access to PII, as allowed within the data protection and privacy framework. (10.2.2)
5. Careful thought should be given to anonymization, since naive approaches to de-identifying data are prone to attacks that combine the data with other publicly available information to re-identify individuals. (10.2.2)
6. Data retention and usage policies should be well-defined, especially for PII. In case the legal framework of the project provides for it, an individual should be able to access data stored in the IT system about themselves, after appropriate authentication of their identity. (10.2.3)
7. The right balance between the individuals right to privacy and the larger public interest should be achieved by the data protection framework. While personal information relating to the individual must be strictly protected from unauthorized access, there may be a need for Government agencies to access or share this data for purposes of national security, economic offenses, tax evasion and other specified circumstances. Hence, authorized sharing of information under specified circumstances, ipso facto, should not be considered as a violation of an individuals right to privacy. However, detailed processes, systems and guidelines need to be put in place to ensure that authorized access and sharing is within the parameters set by law. (10.3)

18

Recommendations for Ministry of Finance projects

18.1. Goods and Services Tax

1. The recommendation of EG-IT for the setting up of an NIU Goods and Services Tax Network (GSTN), for managing the IT systems for GST implementation, including the Common GST Portal is endorsed. GSTN will:

   (a) provide common infrastructure and services to Central and State Governments;

   (b) ensure integration of the Common GST Portal with existing tax administration systems of Central and State Governments;

   (c) build efficient and convenient interfaces with tax payers and tax administrators;

   (d) facilitate, implement and set standards for providing common GST services to the Central and State Governments;

   (e) carry out research, study global best practices and provide training to the stakeholders. (11.2.1.2)

2. The GSTN project may be incubated within NSDL and the preliminary work of conducting a proof-of-concept is being undertaken by NSDL and it has been planned to run a GST pilot with selected State Governments participating in it along with the CBEC. The infrastructure for the GSTN should be based on latest technology and ring fenced, so that whenever the spin-off takes place, the GSTN infrastructure is smoothly transferred to the proposed NIU being set up as GSTN. (11.2.2)

3. The IT strategy document for GST prepared by the EG-IT, which defines the contours of the IT implementation in respect of the GST Common Portal and its interface with all stakeholders, could form the basis for taking forward the implementation of GSTN. (11.2.2)

4. A dedicated Mission Leader and a dedicated Mission Execution Team should be appointed for GST. An implementation team, comprising of officers drawn from and some of the State Governments (pending the appointment of a full-fledged Mission Team and during the pilot stage) should be set up at the earliest. This team would work along with the teams that would be set up by NSDL for implementing the project. The two teams should together initiate the implementation of the GSTN including such as acquisition of necessary infrastructure, design and development of the application, etc. (11.2.3)
5. The personnel selected to man the implementation team should be trained in the tasks mentioned above. Hiring of talent on contract basis should also be explored as necessary. This team should later be part of the Mission Execution Team. This Team should include professionals with technology and legal expertise. (11.2.3)
6. The Agreement with NSDL should be drawn carefully and with clarity. It should include aspects such as financials, responsibilities of the Government side and NSDL at the incubation stage, acquisition of infrastructure, development of application software, ownership of source code, spin-off to the NIU, and the process of transfer of assets (both tangible and intangible). (11.2.4)
7. Though NSDL is assisting the Government in incubating the GSTN, once GSTN is set up as an NIU, the latter may continue to procure services from NSDL in the initial phases of GST implementation, as it considers necessary. (11.2.4)
8. The GSTN may, as and when it commences its full-fledged operations adopt a business-outcome based, per-transaction pricing model. Even during the period when NSDL is providing such services, a similar approach is recommended. (11.2.4)
9. GSTN will develop and operate the Common GST Portal, which will have common minimal functionality, but will be customizable and extensible by various governments. (11.2.5)
10. GSTN will render the following services through the Common GST Portal:
    (a) Dealer registration (including existing dealer master migration and issue of PAN based registration number)
    (b) Payment management including payment gateways and integration with banking systems
    (c) Return filing and processing
    (d) Taxpayer management, including account management, notifications, information, and status tracking
    (e) Tax authority account and ledger Management
    (f) Computation of settlement (including IGST settlement) between the Centre and States
    (g) Processing and reconciliation of import GST and integration with EDI systems of Customs
    (h) MIS including need based information and business intelligence
    (i) Maintenance of interfaces between the Common GST Portal and tax administration systems
    (j) Provide training to stakeholders (11.2.5)
11. The CBEC and State Governments may design and develop their own applications to meet requirements for effective tax administration such as audit, intelligence gathering. (11.2.5)

12. The Common GST Portal is a pass-through device for information, while enhancing it with intelligence to plug leakages. It would also act as a tax booster, matching the input tax credits in the returns to detect tax evasion. It can also integrate with various other systems at MCA and CBDT for verification of PAN or other corporate information and perform data mining and pattern detection to detect tax fraud. It would send this information as alerts and reports to the respective tax authorities. It would also compute inter-State settlement, netting IGST across States. (11.3.1)
13. The following important milestones that would facilitate timely implementation should be kept in view:
    (a) Finalisation of business processes of registrations, returns, and payments
    (b) Commencement of GST pilot project by NSDL with identified States and Centre.
    (c) NSDL to set up core functionalities of common portal in pilot and provide APIs for all stakeholders. Limited testing of APIs by participating stakeholders.
    (d) Engaging with participating entities for pilot including dealers, banks and other Government agencies.
    (e) Completing the impact analysis for GST and initiating steps to align existing tax systems at the Centre and all States for GST. This would include changes to business and IT infrastructure. Timely financial approvals and procurements would also be critical.
    (f) Evaluation of Pilot Project resulting in iterative review of processes and IT implementation.
    (g) Finalisation of detailed project report for actual implementation of GST
    (h) Attaining clarity on NIU engagement and structure of GSTN.
    (i) Creation of GSTN and formalising the involvement of NSDL in GST implementation.
    (j) Finalisation of IGST legal framework and business process.
    (k) Implementing the stakeholder outreach program
    (l) Scaling up to GST implementation with administration and organisational restructuring, and training and testing of applications by tax payers and all tax authorities (11.4)
14. The CBEC has set up data centers to run centralized applications for Central Excise, Service Tax and Customs purposes. With the implementation of GST, these and other facilities should be leveraged to the extent possible. An in-depth study (either by an in-house team or by a consultant) of the reusability of the existing ACES project components should be undertaken and necessary steps should be initiated to refashion the same and integrate it with the GST solution. (11.4)

18.2. Tax Information Network

1. The department is at the crossroads of important strategic decisions as the new Direct Taxes Code is to be operationalized from April 2012, requiring major changes in its application system. Although the existing IT related instrumentalities have served the departments needs admirably it may not be advisable to continue with these diverse implementation methodologies. (12.4.1)
2. Considering that its technology needs are large, dynamic, and sensitive from the point of both, security and privacy, the Department clearly needs a dedicated and efficient NIU type organization to set up, manage and run its IT-related infrastructure on long term basis. (12.4.1)

3. The IT Department should prepare a Mission Strategy Document forthwith along with a time bound roadmap for implementation, and all new initiatives should be implemented only in accordance with this Plan. (12.4.2)
4. As part of the preparation of the Mission Strategy Document,the Department must clearly identify IT-related activities and services that it can actively outsource to an NIU and those which it must necessarily handle departmentally. (12.4.2)
5. ITD should directly handle only matters involving policy making, quasi-judicial decision making, exception handling, risk management and enforcement functions. The IT systems required to assist and enable its functionaries in discharge of these should be set up, managed, and run by an NIU. (12.4.2)
6. There is a strong case for a separate well-capitalised and professionally run NIU to handle the IT-related needs of ITD. This should be set up on priority and in accordance with the recommendations in the foregoing chapters. While ITD should retain Board level strategic control, the NIU should have financial autonomy and operational freedom and its affairs. (12.4.2)
7. Such an NIU would necessarily need services of a few departmental officers as domain experts at different levels to enable it to discharge its mandate. It should therefore be possible for suitable departmental officers to be deputed to the NIU for a defined period while retaining lien on their cadre posts. The relevant Rules may be accordingly modified to enable deputation/secondment of a few officers to the proposed NIU. (12.4.2)
8. The multiplicity of platforms should be replaced by a uniform, holistic, rule-based application matrix so as to integrate all the elements of tax collection process through technology with information seamlessly flowing to the users for informed decision making. (12.4.2)
9. The Ministry of Finance should develop the next generation Risk Information Network to enhance the effectiveness and impact of tax collection using functionalities such as comprehensive taxpayer profiling, trend analysis, pattern recognition, and data mining of the information gathered in IT Department, GST, and Customs systems. (12.4.2)
10. Simultaneously, the IT Department needs to restructure and reorganise the Directorate of Systems and re-define its role as the department's single point interface with the NIU so as to take full advantage of the NIU model. As part of this exercise, it may also re-determine the strength of its technical cadres and restructure the same. (12.4.2)

18.3. Expenditure Information Network

1. The establishment of an integrated Expenditure Information Network can help achieve the following objectives:

   (a) monitoring scheme-wise release of funds and outcomes;

   (b) helping in budgeting, planning and decision making based on the evaluation of all plan schemes;

   (c) maintaining time-series information related to each implementing agency, which will enable in evaluating performance;

   (d) ensuring disbursal of funds to intended beneficiaries;

   (e) ensuring timely disbursal of funds;

   (f) reducing float of funds within the system;

(g) up-to-date and near real-time information on utilization of funds;

(h) monitoring of outcomes up to the last mile; and

(i) transparency in disbursal and utilization of funds by making information available in public domain by way of a transparency portal.(13.1.2)

2. The NIU framework should be followed in setting up the EIN. Aspects such as allocation of tasks between the Government and the NIU, appointment of a dedicated Mission Leader and a dedicated Mission Execution Team may be along the lines of the recommendations contained in this report. (13.2)
3. The relationship between the Government and the NIU may be defined by an Agreement as described in this report.
4. EIN may be incubated as per the recommendations in Chapter 4 of this report. Lessons from the experience of setting up GSTN should be adopted in setting up the NIU for the implementation of EIN. (13.2)
5. The EIN solution should ensure balance between standardisation of features and autonomy of States
6. Appropriate incentives should also be devised for full participation at all levels of Government. (13.2)
7. The Central Expenditure Repository (CER) will handle the information flow. The flow of funds will be managed through the banking system. EIN will track all authorizations and forward electronic instructions to banks, sothat funds move only against actual expenditure to service providers. (13.3)
8. Planning Commission, Ministries, Departments, and Program Divisions can be linked to CER and should be able to monitor the outcomes, utilization and fund status through near real-time availability of information about all entities and programs. (13.3)
9. All the agencies such as State bodies, district bodies, village panchayats, block level bodies, and beneficiaries should have access to EIN with appropriate access controls. These agencies can view the funds sanctioned for them and also update the status of utilization of funds by them. (13.3)
10. For greater transparency, citizens should also have access to a transparency portal and information from the ground can be crowd-sourced. (13.3)
11. All financial information made public through a transparency portal should be machine-readable and format-neutral. (13.3)
12. The EIN project is similar to the GST project in many ways. Some of the processes touch more agencies and involve more steps. The Group recommends that the measures suggested for GST may be suitably adapted for the implementation of EIN. (13.3)

18.4. National Treasury Management Agency

1. The NIU framework as described in this report is recommended for the administration of NTMA. (14.2)
2. As recommended in the Report of the Internal Working Group on Debt Management, NTMA should have a dedicated team to manage its operations. The HR structure for Government teams (consisting of aMission Leader and Mission Execution Team) as recommended in this report should be adopted for NTMA. (14.2)

3. The WG has recommended a solution architecture for NTMA, which may be adopted. (14.3)
4. The WG has also provided detailed steps for incubation, which span legal issues, setting up of IT systems, and change management for transferring the functions from RBI to NTMA. The incubation framework, and creation of the platform described in the WG report may be adopted. (14.3)

18.5. New Pension System

1. In order for a well-ordered and mature pension business to develop in the country,
   (a) All pension and provident fund streams should converge in the medium term;
   (b) Costs to go down dramatically due to competition and economies of scale; and
   (c) Rule-based regulations need to give way to principles / risk-based supervision. (15.4)
2. An enabling legal framework that provides the necessary impetus for NPS should be provided. (15.4)
3. The tax treatment of the NPS also needs to be rationalized to provide for, at least equal treatment with other retirement products and providers. (15.4)
4. There is an imminent need to create a certain level of awareness amongst the NPS subscribers that will eventually empower them to make well informed investment choices to protect and further their own interests. (15.4)
5. As the broader mandate of the PFRDA is to regulate the pension sector in the country, this may eventually necessitate the separation of the NPS administration, including marketing and distribution strategies, from the PFRDA. (15.4)
6. NPS should to create a daily MIS with facts about number of subscribers, assets under management, the breakdown of number of subscribers and assets under management under various heads of Government, the number of switches made by customers from one fund manager to another, the returns of the various schemes of various pension fund managers, and summary statistics about the returns obtained by NPS members. The daily release of this information base is essential for policy analysis and the creation of self-correcting forces.(15.4)
7. NPS needs to create an audit mechanism whereby every year, for randomly chosen customers in a statistically meaningful way, a comprehensive review is undertaken about correctness of data, about whether contributions came in on time, and about whether each member was notified about every contribution. The results of this audit should be released into the public domain. This will yield a regular check upon the quality of performance of NPS. (15.4)
8. There is a need to avoid splitting the functionality of NPS across multiple variants of the same product, since the existence of variants reduce portability for customers and increase cost. (15.4)
9. While significant strides in IT implementation have been undertaken in the NPS, there is a need to further leverage recent technological innovations in e-Governance, banking, and financial networks to develop greater efficient mechanisms that leverage use of IT in an end-to-end manner (15.4)
10. More specifically, initiatives may be taken in the following areas to develop a comprehensive integrated pension administration system:

(a) Enabling linkages with HR and payroll systems of the Central and State Governments to obtain subscriber contribution details, among other things

(b) Revamping and automating all pension administration processes

(c) Re-engineering in the context of the user departments, especially in areas related to Government accounting formations

(d) Providing process linking between Government accounting systems and the pensions administration system

(e) The implementation of these initiatives should be accompanied by extensive skill enhancements, learning and change management efforts, in conjunction with nationwide public awareness campaigns. (15.4)

11. As the Aadhaar implementation becomes ubiquitous across the country, there is a need to establish the platform for linking the Aadhaar with the PRAN number, which can enable Aadhaar-linked KYC for pension scheme enrollment. In this aspect, the NPS should also explore opportunities for future integration with the identification and authentications systems of the Unique Identification Authority of India (UIDAI). (15.4)