



USAID
FROM THE AMERICAN PEOPLE

TAPRII
TECHNICAL ASSISTANCE
FOR POLICY REFORM

EGYPTIAN CUSTOMS IT GOVERNANCE POLICIES AND PROCEDURES

EGYPT TAPR-II: TRADE COMPONENT

August 10, 2006

This publication was produced for review by the United States Agency for International Development. It was prepared by the USAID-funded TAPR II project.

EGYPTIAN CUSTOMS IT GOVERNANCE POLICIES AND PROCEDURES

EGYPT TAPR-II: TRADE COMPONENT

TECHNICAL ASSISTANCE FOR POLICY REFORM II

CONTRACT NUMBER: 263-C-00-05-00063-00

BEARINGPOINT, INC.

USAID/EGYPT POLICY AND PRIVATE SECTOR OFFICE

AUGUST 10, 2006

AUTHOR: WILLIAM ZUELLIG

SO 16

DISCLAIMER:

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

CONTENTS

1.0	INTRODUCTION	1
1.1	PURPOSE	1
1.2	SCOPE	1
1.3	TARGET AUDIENCE	5
1.4	TECHNOLOGY SECTOR OBJECTIVES	5
1.5	CUSTOMS STAKEHOLDERS	5
1.6	BACKGROUND	6
1.7	TECHNOLOGY SECTOR IT SERVICES	6
2.0	POLICIES AND PROCEDURES	8
2.1	ORGANIZATION	8
2.1.1	IT Governance Board	8
2.1.2	Technical Advisory Committee	9
2.2	RELATIONSHIPS WITHIN ECA	16
2.2.1	Technology Sector Services	16
2.2.2	ECA Services Provided to Technology Sector	16
2.3	RELATIONSHIP TO EXTERNAL ORGANIZATIONS	17
2.4	MANAGEMENT, PLANNING, AND CONTROLS	17
2.5	TECHNOLOGY SECTOR COMMUNICATIONS AND RESPONSIBILITIES	16
2.6	KEY PERFORMANCE INDICATORS AND MEASUREMENTS	17
2.7	PROJECT MANAGEMENT	18
2.8	TECHNOLOGY STANDARDS	20
2.9	PROCUREMENT	20
2.10	CONTRACTS AND VENDOR MANAGEMENT	21
2.10.1	Standard Contracts	21
2.10.2	Service Level Agreements	22
2.11	INTERNAL AUDIT	22
2.12	CLIENT SATISFACTION	23
2.13	SECURITY	25
2.13.1	Data Confidentiality	28
2.13.2	Data and Network Security and Encryption	28

2.13.3	Transmission and Transportation of Data and Files	28
2.13.4	Passwords and System Access Controls	29
2.13.5	Remote Access.....	30
2.13.6	Internet Usage	30
2.13.7	Personal Computer Usage.....	30
2.13.8	Software Updates	31
2.13.9	Antivirus	31
2.13.10	Firewalls and Intrusion Prevention/Detection.....	31
2.13.11	System Logs.....	32
2.13.12	Reporting Violations.....	32
2.13.13	Enforcement and Penalties.....	32
2.14	BUSINESS CONTINUITY	33
2.14.1	Disaster Planning and Redundancy	33
2.14.2	Backup/Recovery.....	34
2.14.3	Physical Planning and Protection.....	35
2.14.4	Disaster Recovery Training	35
2.15	EMAIL SYSTEM.....	35
2.16	ASSET MANAGEMENT	36
2.16.1	Asset Management.....	36
2.16.2	Standard Operating Environment	36
2.17	DEVELOPMENT STANDARDS	37
2.17.1	General Standards	37
2.17.2	Development Lifecycle	38
2.17.3	Development Guidelines.....	38
2.18	DOCUMENTATION STANDARDS.....	39
2.19	TESTING AND PROCEDURES	42
2.19.1	Testing Types.....	42
2.19.2	Test Strategy	43
2.20	SUPPORT	44
2.20.1	Support and Help Desk	46
2.21	CONFIGURATION MANAGEMENT AND CHANGE CONTROL	49
2.22	QUALITY ASSURANCE.....	49
2.23	CAREER PLANNING AND ADMINISTRATION	50
2.23.1	Careers	51
2.23.2	Recruitment.....	52
2.23.3	Career Planning and Development (Workforce Planning)	52
2.23.4	Training	52
2.23.5	Performance Appraisal and Counseling (Performance Management)	53
2.23.6	Salary Administration and Promotions	57
3.0	IMPLEMENTATION	58
3.1	HELP DESK IMPLEMENTATION PLAN	58
3.1.1	Plan.....	58
3.1.2	Develop or Procure.....	59
3.1.3	Install Pilot	59
3.1.4	Deploy	59

3.1.5	Help Desk Implementation Time Line	60
3.2	IMPLEMENTATION PRIORITIES	60
4.0	APPENDIX A.....	63
4.1	DATA CONFIDENTIALITY AGREEMENT.....	63
5.0	APPENDIX B.....	65
5.1	LIST OF REFERENCES	65
5.2	CRA VISITS AND MEETINGS	65

1.0 INTRODUCTION

The Trade Component of the Egypt TAPR-II engagement requires development of policies and procedures for IT Governance. These policies and procedures are necessary to guide the new Technology Sector, as a portion of the overall restructuring of the Egyptian Customs Authority (ECA), to achieve management and operational efficiencies.

The policies and procedures contained in this document should support and integrate with policies and procedures that are currently evolving at other areas in the new ECA organization. These other areas may be at higher organizational levels or they may be at the same level as the Technology Sector. Regardless of levels, attempts have been made to write the Technology Sector policies and procedures so that they are a compliment to, and do not conflict with these other evolving policies and procedures.

1.1 PURPOSE

Governance can be defined as the systems by which business entities are directed and controlled. The Technology Sector governance structure specifies the distribution of rights and responsibilities among different participants in the Technology Sector and the overall organization, and spells out the rules and procedures for making decisions and taking appropriate actions. This structure assists the Technology Sector in setting objectives and attaining those objectives and monitoring performance. The policies guide the development of strategy, operations, and allocation of resources in carrying out the responsibilities of the new Technology Sector organization. The key issues facing the Sector are how to manage risk, how to provide services at a reasonable cost and efficiently, how to provide security in all activities, and how to control and manage the IT environment within a changing environment. The purpose of this paper is to present those policies and procedures that will allow the Technology Sector to achieve these results.

Formal and consistent policies and procedures will clarify responsibilities, ensure greater consistency of system implementations, reduce problems experienced by users, improve reliability of systems, minimize inappropriate or unauthorized use of systems, protect systems against security threats, and enhance the capability for disaster recovery. They will focus on who makes decisions, and who is held accountable for results.

1.2 SCOPE

Policies should follow the mission statement and the objectives of the organization. In the absence of a mission statement for the Technology Sector, the following will be offered as a draft: "The Mission of the Technology Sector is to provide modern, flexible, effective, and cost-efficient IT services to the ECA". Implicit in this statement is the need to have organizational policies that are not hindered by changing technologies, organizational changes, or changing services.

In addition the stated ECA's organization realignment's objectives are:

- "To create a modern, flexible and responsive Customs organization that supports Egypt's trading capacity and provides effective and efficient protection for Egypt's borders".

- “Provide the platform for re-engineering and modernizing ECA Customs law, procedures, and processes”.

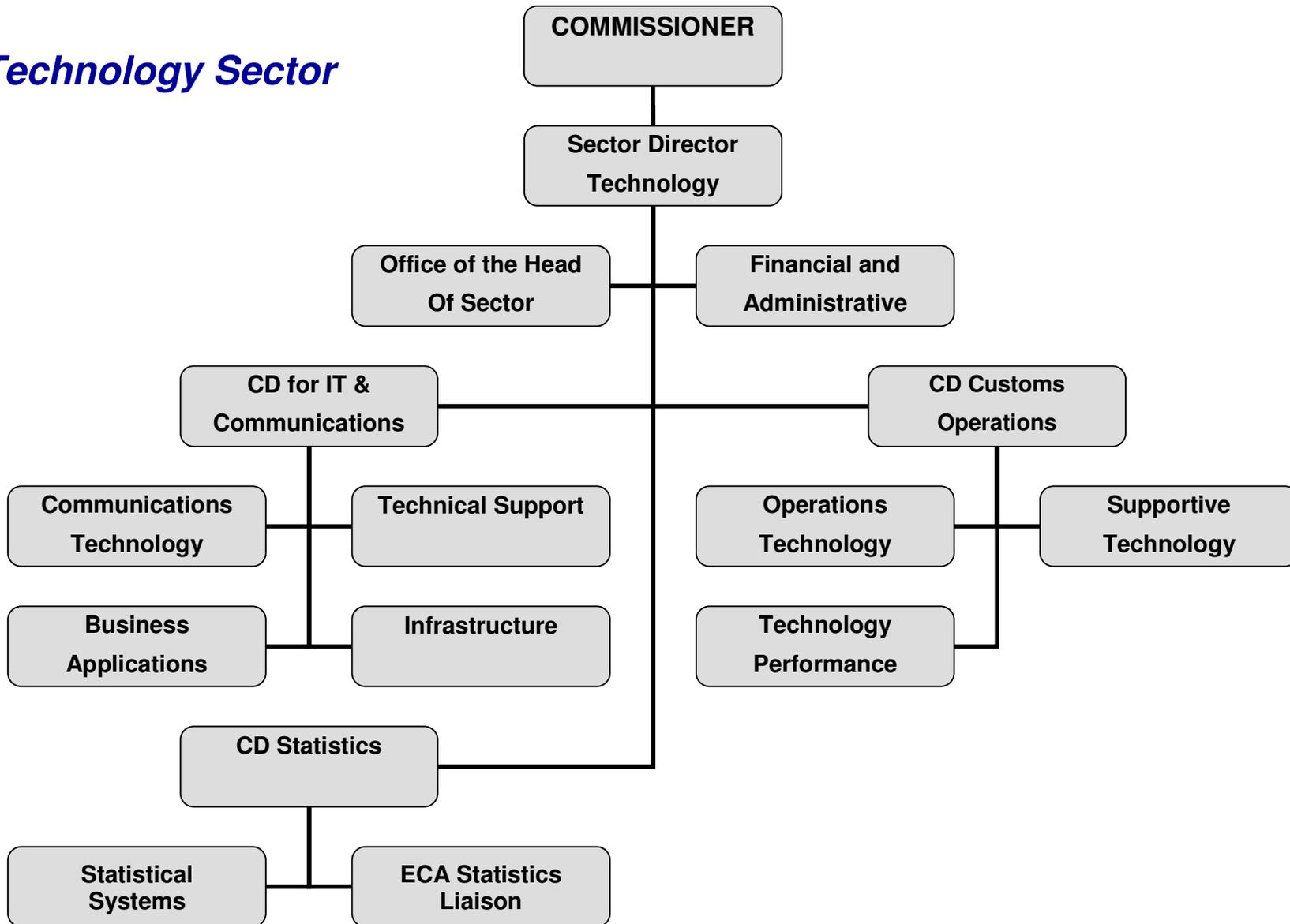
The statement of policies and procedures covers all of the proposed organizational units within the new Technology structure headed by the Sector Director of Technology. However, the emphasis is on those areas that involve or affect information technology rather than non-IT technology areas. Policies provide the Sector-wide direction that guides the Sector in making business decisions. These help ensure compliance with applicable policies with the ECA, promote operational efficiencies and reduce risk.

Procedures consist of a set of guidelines or description of steps which when followed, implement policy. Procedures draw their authority from policies or other procedures.

Policies and procedures will be written, and will be maintained using configuration controls and standards used in other documentation within the Technology Sector. They will be disseminated under the signature of the Sector Director Technology. Policies and applicable procedures will be reviewed with all Sector employees annually.

The proposed Technology Sector organization that is addressed in this document is shown in the following chart:

Technology Sector



The policies and procedures in this document will address the following organization boxes:

- Sector Director Technology
- CD for IT and Communications
 - Communications Technology
 - Technical Support
 - Business Applications
 - Infrastructure
- CD Customs Operations Supportive Technology (as it pertains to IT technologies)
 - Operations Technology Initiatives
 - Technology Performance Monitoring
 - Supportive Technology Maintenance and Administration
- Financial and Administrative Affairs
- Office of the Head of the Sector

Those areas outside of IT technologies, such as X-ray, electrical equipment, etc., are generally not included in the policy and procedure statements. However, many of the policies and procedures are written broadly enough so that they may be adapted to these non-IT areas.

The scope will include functional areas within all of the above organizational units. These functional areas address:

- Organization and reporting structure
- IT Governance Board and Technical Advisory Committee
- Management, planning, and controls
- Key performance indicators and measurements
- Relationships within the ECA
- Relationships to external organizations
- Project management
- Technology standards
- Contracts and vendor management
- Procurement
- Internal audit
- Client satisfaction
- Security
- Email system
- Asset management
- Development standards
- Documentation standards
- Testing
- Technical Support
- Configuration management and control
- Quality assurance
- Career planning and administration

1.3 TARGET AUDIENCE

This document has been prepared primarily for the Egyptian Customs Authority and the Customs Reform Unit. It will also be read by USAID and other consulting and donor organizations.

1.4 TECHNOLOGY SECTOR OBJECTIVES

The objectives of the Technology Sector are to provide improved service levels for the new business organization, and to bring increased customer satisfaction to the ECA. The Technology Sector will utilize architectural solutions that follow current leading practices for similar Customs organizations world-wide. The Sector is to explore new value-added services such as outsourcing where appropriate in order to reduce cost, and improve services to all of its clients. It will assure security, privacy, and accountability in its services and how it processes data.

Its systems will scale to meet the demands of additional growth in traffic and applications. It will provide high availability and transaction integrity. It will provide automation integration wherever possible. It will minimize the complexity of development and maintenance through the use of 3rd parties, and by maintaining a Sector core group of skilled personnel.

1.5 CUSTOMS STAKEHOLDERS

There are numerous stakeholders that have an interest in the ECA IT systems and computing environments. The policies and procedures will apply, to some degree, to all of these various stakeholders. The primary stakeholders include or will include:

- Egyptian Customs Authority (ECA)
- General Office for Export and Import Control (GOEIC)
- Ministry of Finance (MoF)
- Traders/Importers/Exporters
- Freight Forwarders/Brokers
- Manufacturers
- Port Authorities (both Public and Private)
- General Authority for Free Zones and Investment (GAFI)
- General Deposit / Warehouses
- Ministry of Trade and Industry
- Ministry of Economy
- Ministry of Health
- Ministry of Agriculture
- Ministry of Foreign Affairs
- Chambers of Commerce
- International Transport Union
- Foreign Customs Administrations

1.6 BACKGROUND

Policies and procedures are required to provide both longer term as well as daily guidance for the Technology Sector in how they perform their tasks. The policies and procedures described in this document are a draft that will evolve and change, as ECA policies and procedures are defined in different departments and sectors within the ECA. The scope of the policies and procedures in this document is limited to the IT related portions of the Technology Sector.

Attempts have been made to recognize that the policies and procedures in this document will have to eventually integrate with and compliment those in other Sectors whose policies and procedures have yet been drafted. The Sector for Security, Finance & Administration Services, Central Directorate for Security Service, is an example, where its policies and procedures must eventual link and integrate with what is being drafted for the Technology Sector. Specifically, within the Central Directorate for Security Services, there are several departments that have obvious policy and procedure links with the Technology Sector. As their polices and procedures evolve these need to be linked with and complimentary to those being drafted for the Technology Sector. At the time this document was written, drafts of other sectors' policies and procedures were not available. It should be noted that the policies and procedures in this document are not meant to dictate or place constraints on the other sectors drafting of policies and procedures. Technology Sector's appear to be some of the first being drafted, and as such, they may have to be revised as other sectors policies and procedures are drafted.

The "Egyptian Customs Authority Organizing for the Future" document was used in determining the structure of the new ECA. A number of interviews were conducted with Technology personnel and ECA advisors in order to understand the current organization, its capabilities, and to help envision how the new Technology organization will evolve. Extensive time was spent with Mrs. Iman El Kouny, Executive Consultant Customs Reform. Mrs. El Kouny provided valuable guidance and insight on the new organizations; she also provided reviews and advice on the drafts of this document. Mr. John Yates of BearingPoint provided consistent guidance and reviews of the draft documents, as well as background information. The "Egyptian Customs Interim Modernization Phase IT GAP Analysis" document, produced by Mr. John Yates of BearingPoint in February, 2006; and also the "Egyptian Customs Strategic IT Security – Infrastructure Analysis and Recommendations" document, issued by BearingPoint on June 22, 2006, has been used in this document, and have been very helpful in defining client types, components of infrastructure, and security or processing zones.

The Technology Sector as envisioned in the new organizational structure, will have many similar functions to what is has today. What has changed is the degree to which it will concentrate on IT and other technologies, and the need to become a professional technology organization with professional management, and highly motivated and technically competent individuals. The current number of technical personnel as stated in the February 2006 GAP Analysis previously mentioned, must be supplemented by a substantial number of trained technicians. Policies and procedures must be developed to allow these individuals to understand their responsibilities and to allow management to measure the performance of individuals and organizational units.

1.7 TECHNOLOGY SECTOR IT SERVICES

In order to write policies and procedures, the services offered by the Sector need to be defined. These include but are not limited to:

- Processing for Customs core functions such as manifests, declarations, maintenance of tariff tables, tracking and clearance of cargo, inspection status
- Processing amounts due and payments including electronic payments
- Data exchange with GOEIC and other governmental agencies
- Trade Web services
- Developing and maintaining public website information

- Email (limited at this time)
- Processing of temporary admissions
- Providing internal and external client support services
- Providing application systems for internal users for risk management, reporting, statistics, measurements, performance, personnel, purchasing budget, supplier and payroll
- Maintaining electronic archives
- Providing end-user training on the use of Customs systems
- Maintaining hardware, software, and data networks
- Providing Help Desk, first and second line technical support
- Managing vendors that provide maintenance services
- Providing guidance to user organizations in usage of and planning for IT systems
- Providing guidance, planning and support services to executive management in project management, cost effective IT solutions, and costs for alternative offerings.
- Providing costs estimates and budget estimates to assist Financial Planning
- Providing secure information processing and secure physical environment

2.0 POLICIES and PROCEDURES

The policies and procedures in this document will be stated for the organization in general, and then for a number of organizational units within the Technology Sector, and finally for specific functions within the Sector.

The policies and procedures will enable the Sector to improve its performance through proficient collaboration of people, processes and technology in the domains of:

- Strategy
- Sourcing
- Architecture
- Program management
- Development
- Quality

The policies and procedures will assist the Sector in aligning IT direction and resources, prioritizing projects, delivering results as promised, and finding the right balance between efficiency and service.

2.1 ORGANIZATION

The Technology Sector provides services and support to other ECA and non-ECA organizations. In its role as a service provider to a variety of clients, it must ensure that it coordinates its objectives, projects, policies and procedures with these other clients.

Two boards or committees are recommended to provide this guidance and corrective actions to the Sector. The first is the IT Governance Board, which currently exists and provides broad overall guidance and direction, as well as program management for large systems investments. The other and new one is the Technical Advisory Committee (TAC), which will provide shorter-term guidance, with an emphasis on technology and its applications.

The Technology Sector will receive direction and guidance from the IT Governance Board and the TAC in the areas of strategy, tactical operations and planning, project management, and technology.

2.1.1 IT Governance Board

IT Governance Board is a high level board that provides strategic direction to the Technology Sector. Some or all of its functions may eventually be performed by the Strategic Directorate.

The IT Governance Board will provide long-term and mid-term guidance to the Technology Sector. It will monitor large projects, prioritize planned projects, and ensure that resources are in place for approved large projects. It will receive requests and recommendations from the Technology Sector, other Sectors, and the IT Technical Advisory Committee. It will function as the overseer of major

projects and plans for the Technology Sector, and provide guidance and advice for smaller projects when requested.

The IT Governance Board confirms that the business strategy and the business requirements are linked directly with the objectives of the ECA. The Board should determine the technology implications of the business requirements, understand the risks, and ensure that the selected solution is both feasible, cost effective, and within the risk profile established by the Board. The board should insist on reviewing conceptual designs and business cases.

The IT Governance Board should determine the type of sourcing for a major project. This will determine whether the development or other efforts are done within the ECA Technology Sector or by vendors and 3rd parties including outsourcing. This requires that sound business cases be developed including detailed costs estimates, benefits, identified risks, life cycle costing, and alternative solutions.

The IT Governance board should:

- Annually should request an IT Strategic and Plan from the Technology Sector.
- Evaluate Technology major project requests from ECA sectors and the TAC.
- Align IT direction and resources for major projects.
- Request additional project definition including objectives, scope, benefits, required budget, resources, timeframes, and risk analysis.
- Coordinate project requests with the various affected organizational units within the ECA and external to the ECA.
- Prioritize projects and allocate resources to projects.
- Provide overall project management, monitoring and control.
- Request monthly and ongoing project status.
- Request periodic updates on new and emerging technologies and their potential benefits to the ECA.
- The Technology Sector should have a voting representative on the IT Governance Board.

2.1.2 Technical Advisory Committee

IT Technical Advisory Committee is comprised of members within the Technology Sector and the ECA, plus other government agency and external IT technology experts. Its purpose is to provide guidance on technology strategies, direction, and procurements. Both internal and external customers will be represented on this Technical Advisory Committee. Its recommendations will be presented to the IT Governance Board for their review and potential inclusion in the overall technology plan.

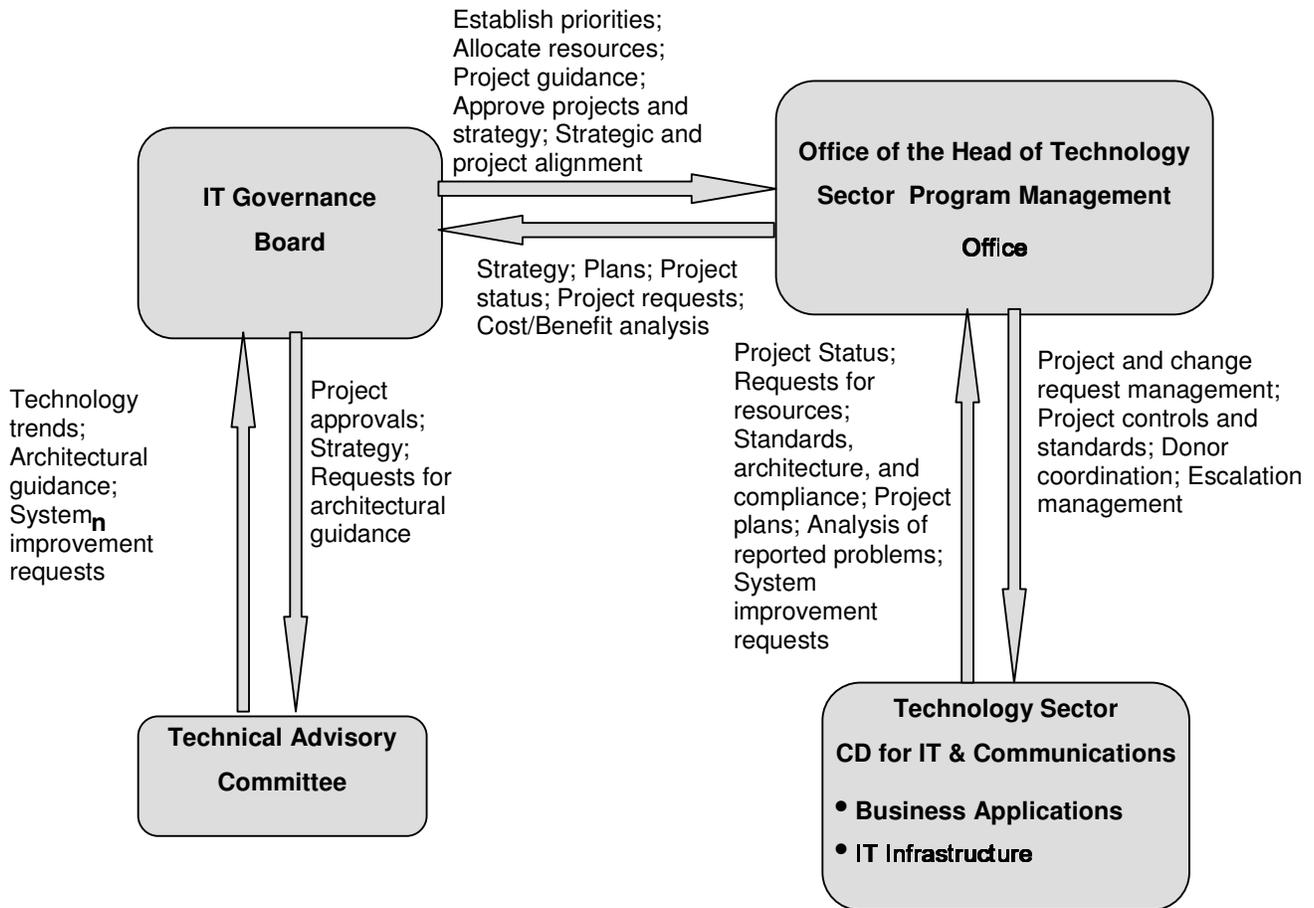
The TAC is to:

- Provide technical guidance to projects and to the IT Governance Board
- Review projects plans and require risk assessments on key technology portions of the projects
- Request and evaluate solutions to minimize technological risks
- Be a formal mechanism for major system change requests, recommend acceptance or rejection, and provide priorities to those accepted.
- Review Technology Sector use of technologies to ensure they are current and are cost effective.
- Membership in the TAC should be defined by the Sector Director of Technology. It should include executive level personnel from representative ECA user communities, both internal and

external. It should include technical representation from the Technology Sector and outside organizations such as other Ministries and IT experts.

The following diagram summarizes the primary relationships between these entities, and the Technology Sector.

Relationship of IT Governance Board and Technical Advisory Committee with Technology Sector



Coordination of Technology Sector, and Governance Board and /Technical Advisory Committee:

- **IT Governance Board has strategic, large project responsibility**
- **Technical Advisory Committee has large system change requests, technical and architectural advisory, and system problem and performance issues advisory responsibilities**
- **Office of the Head of Sector Program Management Office has project management, project controls and standards, and interface with IT Governance, reporting responsibilities**
- **Business Applications and IT Infrastructure Departments have responsibility for designing, implementing, and supporting systems and infrastructure; reporting project status; analyzing problems and recommending solutions.**

2.2 RELATIONSHIPS WITHIN ECA

In terms of policies and procedures the Technology Sector has specific relationships with other sectors and departments within the ECA, beyond those previous discussed in section 2.1. These other organizational units use Technology Sector services and support; or provide strategy, planning, and direction to the Sector.

2.2.1 Technology Sector Services

Technology Sector provides services and support to other organizations. Its policy is to be responsive to requests and changing needs, subject to budget and priority constraints. User requests and needs will be formally communicated to Technology Sector through a number of mechanisms. The primary feedback mechanisms and the means to initiate new major systems, major enhancements to existing systems, system improvements come from:

- IT Governance Board
- IT Technical Advisory Committee
- Client Satisfaction Survey
- Analysis of Help Desk and Support problems and requests

Each of these has or will be discussed in further detail.

It is the policy of the Technology Sector to continually involve users in the entire lifecycle of IT projects. This starts with an idea of a conception of how IT can solve a business problem through the development of the solution, and finally to the implementation and post-implementation support of the solution. Technology Sector will encourage users to take ownership of defining functional and training requirements, performing user acceptance testing, writing and documenting user procedures, developing user training materials, and in reporting functional and system problems.

2.2.2 ECA Services Provided to Technology Sector

A number of ECA Sectors provide services, support, strategy, planning and direction to the Technology Sector. Strategic Planning & Initiatives Sector provides a long-range plan for ECA; the Strategic Planning & Initiatives Sector will review Technology Sector's yearly and multi-year plans and ensure that it fits into the overall ECA plans and objectives.

The Human Resources & Capacity Building Sector will define generic positions and training, recommend training and delivery mechanisms, and provide recruitment services to the Technology Sector. Technology Sector will utilize these generic positions by refining them to fit the unique positions' technical requirements. The same procedure will be followed for specific IT training, where Human Resources & Capacity Building Sector will define the generic training; Technology Sector will refine these to add fit its unique requirements. Human Resources & Capacity Building Sector must approve the Technology Sector's refined positions and training requirements.

Security, Financial & Administrative Services Sector will provide support services to the Technology Sector. These includes facilities; procurement; archiving and retention of documents; budget and forecast; physical security guidance; document recording and tracking; and physical document custody policies and procedures. Systems data and information transmission and security are the responsibility of the Technology Sector. Technology Sector will work with the Security, Financial & Administrative Services ensure that its policies and procedures are complimentary and not in conflict with the ECA's broader policies and procedures. Technology Sector will submit its draft of yearly

and multi-year budgets to Security, Financial & Administrative Services Sector as part of the annual budget preparation procedure.

2.3 RELATIONSHIP TO EXTERNAL ORGANIZATIONS

Technology Sector provides services and support to a number of external organizations, including GOEIC, other Government of Egypt (GoE) agencies or Ministries, private companies, international organizations, non-governmental organizations, and the general public.

It is Technology Sector policy to be responsive to these organizations' requests and needs as they pertain to ECA information systems.

The formal means of communication with external organizations is through the same four mechanisms used for internal organizations. These are:

- IT Governance Board
- IT Technical Advisory Committee
- Client Satisfaction Survey
- Analysis of Help Desk and Support problems and requests

The IT Governance Board may have external organization representation. The IT TAC will have members representing external organizations. The Help Desk and the technical support organization receive reports of problems, from which repairs, recommended improvements on system performance, support performance, functional system enhancements, and requirements for new business functional areas may be addressed. The analysis of the major problems and requests will go to both the TAC and the IT Governance Board for review, discussion and disposition.

2.4 MANAGEMENT, PLANNING, AND CONTROLS

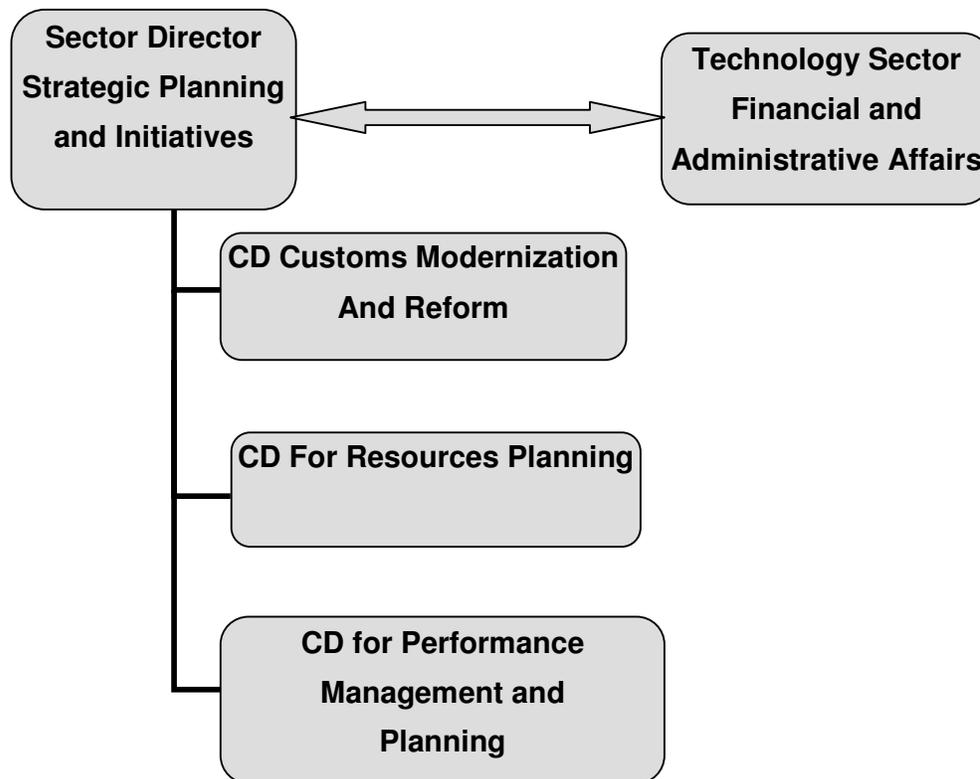
The Technology Sector's objectives, plans and priorities will be driven by the ECA Strategic Plan. The IT Governance Board will provide guidance and direction, identify and oversee major projects, and approve resources to the Technology Sector in order to complete these major projects.

Technology Sector should focus on managing, planning, controlling, servicing, and supporting the current production systems, those that are currently in development, and those planning to start within the next 2 years.

Technology Sector's planning cycle will be tactical in nature, not more than 2 years out. An annual plan, extending for 2 years, should be submitted to both the IT Governance Board, and to the Strategic Planning & Initiatives Sector for approvals. Technology Sector's communication with the IT Governance Board is done through its representative on the Board and formal communication with the Board.

Technology Sector will coordinate its plans through its Financial and Administrative Affairs Directorate (F & AAD), with the ECA's Strategic Planning and Initiatives Sector which is responsible for overall ECA strategic planning. Technology Sector will collect and provide capital outlay amounts, depreciation costs, expensed costs, and direct labor charges to Central Directorates within the Strategic Planning and Initiatives Sector in total or by project as required. The following diagram illustrates the key areas that Technology Sector will coordinate its activities with the Strategic Planning and Initiatives Sector, includes Central Directorates for Modernization and Reform; for Resources Planning, and for Performance Management.

Technology Sector Coordination with Directorate for Strategic Planning and Initiatives



Coordination of Technology Sector and Strategic Planning and Initiatives Sector

- Program and Project Planning
- Coordination with Donors
- Strategic Planning and 2 Year Plans
- Guidance on International Best Practices
- Workforce Planning

The Technology Sector will produce a plan annually that covers a 2 year period. It will include planning for:

- Alignment with ECA plans and priorities
- Requested budget for capital and ongoing expenses
- Personnel and salaries
- Job positions and number of personnel in each position
- Computer hardware, network equipment, and software
- Contractor and other 3rd party requirements
- Training
- In process projects and approved projects to start within 2 years
- Annual Security and Risk Mitigation Plan

2.5 TECHNOLOGY SECTOR COMMUNICATIONS AND RESPONSIBILITIES

The Technology Sector must ensure that communications and responsibilities within the Sector are clearly understood and followed. The following is a list of the key responsibilities and how communications is made with other departments within the Sector. Responsibilities of the Sector Director of Technology, Financial and Administrative Affairs, and Central Directorate Operations Supportive Technology are:

- The Sector Director is responsible for approving all system and infrastructure requests. Egyptian pound and/or person-days of labor effort limits should be established as cutoff points, below which the Sector Director can approve and implement; above which he must submit to the IT Governance Board for approval.
- Procurement requests may be initiated by Business Applications, IT Infrastructure, Communications Technology, Technical Support, Operations Technology Initiatives, and CD Statistics. These are sent to Financial Administrative Services Procurement to ensure they have been defined, have estimated costs, and fit into the overall Sector plan. Once approved they are then sent to the Central Directorate for Administrative Services to ensure the procurement request is within the planned budget. Technology Sector Financial and Administrative Affairs are responsible for managing the delivery, installation, and post-installation performance of the vendor.
- Project management and coordination of major projects with 3rd parties, NGO's, and donors should be done by the IT Governance Board. The Sector Director of Technology is responsible for implementing those projects approved by the IT Governance Board, and reporting progress to it. The Sector Director has a project management role to plan and manage those portions of major projects that fall within the Sector's responsibility. A small project office should be setup within the CD for IT & Communications or in the Office of the Head Of Sector to coordinate, collect, report, and manage information for these large projects.
- Operations Technology Initiatives Department in the CD Customs Operations Supportive Technology is responsible to ensure that changes in department level functions are identified. This includes defining new roles within departments that will be needed as a result of changes. Some of the activities that will be addressed are:
 - Identify Sector objectives, measurements and controls
 - Define functions performed by the Sector
 - Measure performance of the plans and report the results to the Technology Sector Director
- Financial and Administrative Affairs is responsible for maintaining work procedures and guidelines, and for developing and maintaining standard operating procedures.
- Financial and Administrative Affairs is responsible for coordinating career development, employee evaluations, training, procurements, budgets and liaisons with other Sectors regarding administrative and financial matters.

Those responsibilities that largely are in the departments in the Central Directorate for IT & Communications are:

- Delivery of new application systems and system enhancements is part of Business Applications.
- Delivery of support services is in the Technical Support Department.
- Delivery of requirements and service requests are within Business Applications Department. Technical Support collects requirements, analyzes and consolidates them, and passes new requirements and application requests to Business Applications. Business Applications consolidates these requirements with ones they get directly from clients, works with the IT Infrastructure Department to ensure that infrastructure needs are in the plan, prepares cost/benefit analysis, perform make versus buy analysis, and recommendations that go to the Head of IT & Communications for approval. All of these tasks are planned and monitored for the Project Management Office. After approval these go to the Sector Director and the Office of the Head of the Sector for approvals, and if sufficiently large are forwarded to the IT Governance Board for their review and approval. Once approved these requirements are incorporated into a plan which is sent to the Operations Technology Initiatives Department for incorporation into the Sector's overall plans.
- Integrated project management through a project management office established in the CD for IT & Communications or in the Office of the Head Of Sector.
- Help Desk and Frontline support is provided by Technical Support. They record problems and perform periodic analysis of problems, and look for repeat problems that can be submitted to Business Applications and IT Infrastructure for additional analysis and resolution.
- Infrastructure support, for hardware, networks, and system software is provided by IT Infrastructure. They receive problem notices from the Help Desk. They initiate scheduled configuration controlled updates to infrastructure. All infrastructure upgrades and fixes are sent to the Business Applications department for approval prior to implementation to ensure that these are tested against applications and will not cause problems once implemented.
- External client support is provided through the Help Desk in Technical Support, which communicates problems and requests to IT Infrastructure or Business Applications.
- CD for IT Communications provides guidance to executive management for cost effective IT solutions, alternative solutions, costs and benefits.
- User training is provided by Business Applications. User training needs are determined through analysis of Help Desk and Support reported problems, the introduction of new application systems, and functional changes to existing application systems. Business Applications should move toward a "train the trainers" role, where they train key end-user personnel so that these key personnel can perform most of the ongoing end-user training.

2.6 KEY PERFORMANCE INDICATORS AND MEASUREMENTS

The policy of the Technology Sector is to establish clear performance indicators that will be measured against actual results. Measuring the results against the indicators will help direct or redirect the Sector's efforts, indicate where resources are required to resolve ongoing issues, and will become a vital input to individuals annual performance review.

Technology Sector will be measured in the following areas:

- Client satisfaction with services and support with an overall rating of 3.5 in year 1 on a scale of 0 to 5, 5 being the highest. By the end of year 2, the client satisfaction should be 4.0.
- Per cent system availability measured against a target of 98% available for each node, over a 24 hour 7 days per week period.
- System response time for online transactions, no more than 5 seconds. The calculation is the number of responses greater than 5 seconds compared to all responses. The target is 2% or less over random 24 hour periods.
- System restoration time after a major outage, a maximum of 2 hours.

- Outstanding production problems and time to resolve the problems. The target is to have level 1 problems resolved with 2 hours; level 2 within 1 business day; level 3 within 3 business days. The measurement is the % of problems not resolved within these limits compared to the total number of problems reported for each category. The % is each level is 98%.
- Cost-effective delivery of services by staying within the approved budget.
- Promotion of personnel and skills enhancement. The actual number of promotion and the skills enhanced during the year should be compared with the targets specified in the annual Personnel Plan. The target is to make 100% of the plan.
- Number of security violations. These should be counted and categorized as critical, severe, and minor. All 3 categories should be divided by the total number of security violations. The targets are to have no more than 3% critical; 20% severe and 77% minor.
- Annual evaluation by the IT Governance Board on the effectiveness of the Technology Sector. The measurement is quantitative and subjective. In general the annual evaluation should be constructive of the Technology Sector.
- How well the IT Annual Plan, as approved by the IT Governance Board, has been implemented during the year. This is a subjective measurement; however individual project's performance can be measured against the plan in terms of cost, time, quality, and key deliverables.
- Performance of vendors and outsourcing companies against Service Level Agreements (SLA). The measurement is for all vendors and outsourcing companies to perform 100% against their respective SLA's in all categories defined in the SLA's.
- The Sector has a department responsible for Strategy and Planning, under the Operations Supportive Technology Directorate. It should be responsible for establishing the quantitative and qualitative benchmarks for the above, and collecting the statistics necessary for measuring actual results against the benchmarks. The measurements against benchmarks should be done quarterly and the findings presented to the Sector Director Technology.

2.7 PROJECT MANAGEMENT

Project management establishes best practices for the management oversight that guides projects to success. Project management should be employed by all departments within the sector, with special emphasis on those departments that design, develop, implement and support systems. These departments primarily are in the CD for IT & Communications. Project management functions include working closely with the IT Governance Board to ensure that:

- Project are well defined
- That there is an owner of the project with authority to commit resources and timeframes
- That the project has proper planning, management and controls
- That there is an approve budget
- There is sufficient information to make the buy versus build decisions, and to commit to major procurements

Project management is the formal processes and procedures used to manage all Sector IT projects. Project management includes:

- Developing a project plan with tasks, timelines, budget, assigned resources, deliverables, and milestones
- Developing a tracking and monitoring plan that will show progress, detect problems, and allow for corrective actions
- Utilize a system development methodology that defines standard phases, activities, tasks, and deliverables
- Define project ownership
- Develop and implement change control, by establishing distribution procedures for software and hardware changes, and version controls

- Ensure quality control and assurance over the project management processes and over the activities and tasks performed in the project
- Establish formal reporting procedures for status reporting, costs, management reviews, and issues and problems
- Coordinating the activities of ECA, Technology Sector, vendors, other GoE agencies, 3rd parties, NGO's, and outsourcers from one consolidated project plan

Many if not all projects overlap multiple departments. It is the policy of the Technology Sector to have a Project Management Office (PMO) in the CD for IT & Communications or optionally in the Office of the Head Of Sector, which is responsible for overall management of these multi-department projects. The PMO's responsibilities, which can be delegated to other areas with the Sector such as Quality Assurance include:

- Define ownership of projects
- Develop project schedules, resources, and plans
- Establish the change management processes to be followed in the Sector
- Establish standard development environments
- Coordinate procurement of all system resources (development, test, production)
- Provide project management of all major projects
- Ensure development lifecycle standards are followed
- Conduct requirements analysis
- Collect reporting of project progress against the plan, measure performance, identify problem areas and discrepancies against plan, and recommend corrective actions.
- Communicate project progress, status, plans and actions to all affected organizational units (centralized reporting)
- Escalate problems and issues
- Conduct design reviews
- Ensure all testing is completed
- Develop training plans and documentation
- Maintain project repositories
- Develop plan for change management
- Develop deployment and support plans
- Ensure all system documentation is compliant and complete
- Link problem reporting and the need for new system requirements

The PMO should function as the organization within the Sector that ensures the priorities established by the IT Governance Board are being adhered to. The PMO can provide governance and project management over all projects. The PMO will direct and provide guidance to other departments within the Sector for the information it needs to manage and report project progress. This includes working closely with Quality Assurance department.

The PMO should coordinate the IT efforts with outside entities such as donors, and other GoE organizations. The structure employed should flow down from a higher level within the ECA, where the donors and other organizations have representation on advisory or other committees.

The PMO should be the central collection point for all requests for system improvements, changes, and new applications. These requests will originate with users, come from the analysis or system problems, be requested by Business Applications or Infrastructure departments. The PMO will assist or prepare requests for a system improvements or a new application request.

The PMO should ensure that contracts written for software vendors have the Sector's provisions for System Development Lifecycle Methodologies; project management and controls; project reporting;

well –defined and measurable deliverables; testing requirements; defined acceptance criteria; documentation; training; and a support plan.

2.8 TECHNOLOGY STANDARDS

Technology standards will be developed in order to utilize only current and known technologies, and to limit the number of technologies in order to reduce maintenance costs. Widely used and known technologies, supported by international standards should be used.

An objective of limiting the number of technologies is to limit the number of maintenance and service providers, to minimize spare parts costs, and to make contract management more manageable and measurable.

Technology standards will be established based on the current System Operating Environments (SOEs) and the known technology requirements of the Sector within the next 2 years. The standards will change as new major software systems such as the new CCAA are implemented and require different technology than are currently used.

Technology Sector will stay current with hardware technology where possible. It is more important for consistency in procuring computer technology by utilizing standard operating environments (SOEs), than trying to keep up with every technological advance in hardware or software. New technology should be considered for incorporation into the SOEs only after they have entered the market place and have been proven to offer a measurable improvement over prior technologies.

Specific current or emerging technology standards that should be utilized are:

- XML in particular for data exchange
- Relational database management systems, Open Database Connectivity (ODBC) compliant and have database replication capability
- Utilize current Linux, Microsoft, and Unix operating systems
- Utilize Microsoft Windows for clients
- Utilize a standard office automation software such as Sun Star Office or Microsoft Office
- Standardize on one or two network component vendors for switches, routers, firewalls, intrusion prevention appliances, authentication/authorization/accounting appliances.
- Standardize on one, two or three security software product vendors in order to maintain security integration across various hardware and software platforms.
- Standardize on two or three computer hardware vendors in order to minimize maintenance agreements and warranty issues
- Standardize on one antivirus enterprise level software product
- Standardize on preferably one, and at most two development suites of software

2.9 PROCUREMENT

Technology Sector will develop technical requirements, issue RFP's, evaluate proposals, select winning vendors, and manage the delivery and installation of procured equipment, software and services. They will coordinate their efforts with Finance & Administrative Central Directorate for overall guidance on procurement policies and procedures. The Sector will follow the procedures as established by the Finance & Administration Central Directorate for open competition and other Request for Proposal procedures.

Procurement of equipment will utilize the Standard Operating Environments (SOEs) as the baseline for specifying the requirements. These may be altered with Director of Technology Sector's approval.

Procurement activities will be coordinated by the Sector Financial and Administrative Affairs department. They will ensure that the tracking and reporting of progress against a procurement plan includes activities for:

- Procurement performance, technical, quality, delivery, and maintenance specifications
- Vendor evaluation and selection
- Shipment and delivery
- Installation of equipment
- Training
- Warranty and maintenance support

2.10 CONTRACTS AND VENDOR MANAGEMENT

All contracts originating in the Technology Sector are to be coordinated through the CD for Financial & Administrative Services, Procurement & Warehousing Directorate. Standard contracts for the ECA are defined by these organizations. The Technology Sector will use these standard contracts, modify and add to them as required, and then submit these to Procurement & Warehousing for approval.

Technology Sector should develop the procurement requirements, develop the evaluation criteria for technology procurements, assist in writing and evaluating requests for proposals, assist in vendor contract and terms negotiations, and work closely with vendors in post-installation maintenance management.

2.10.1 Standard Contracts

Standard contracts should contain at a minimum:

- Purpose of the contract
- Definition of the scope of procurement of hardware, software, services, or other as a Statement of Work
- Project schedule including tasks, milestones, responsible organization, and time frames
- Deliverables
- Delivery schedules
- Length of time of the contract
- Invoicing and payment schedule
- Service Level Agreement
- Description of non-compliance, penalties and enforcement for non-compliance
- Ownership of materials related to services
- Responsibilities of all parties signing the contract
- Warranties
- Termination and Indemnification
- ECA confidential information and security procedures
- Change Order procedures
- Dispute resolution

All maintenance contracts should specify the need for disaster recovery and require that vendors specify how they will accomplish this.

2.10.2 Service Level Agreements

The Sector will develop Service Level Agreements (SLA) for development, operational, and maintenance contracts. SLA's define the roles, responsibilities, and objectives in a support agreement. A SLA may include any or all of the following, depending on the types of services or deliverables:

- What will be delivered, when, and what procedures to follow for delivery, configuration management, issues tracking, etc.
- Standards used to produce, document and deliver the service or deliverable
- How many vendor certified or qualified technicians are to be available for support activities
- What specific maintenance performance indicators will be measured
- Satisfaction criteria (e.g. end-user satisfaction resulting from a survey)
- Availability of service, over what period of time, how measured (e.g., hourly, daily, weekly), metrics in % or time or numbers, and how the service is defined
- Activity, monitoring, and performance reports required from the vendor
- Specify how often monitoring of services, such as network performance, are to be recorded
- How to (methods for) report problems, and the reporting, tracking, and feedback mechanisms for problems
- Response time of reported problems and resolution time for a reported problem. In the case of systems support, this should be reported in categories such as:
 - time for initial response, typically within 1 hour for a server or critical network component
 - time for onsite response, typically 2 hours for a server or critical network component
 - time to fix or determine escalation, typically 6 hours for a server or critical network component
 - time to fix after escalation, typically no longer than 3 days
- Escalation procedures and what triggers escalation for service, with defined levels, time to respond, and user notification procedures. Escalation should be based on a combination of the type of failure, number of users affected and the time to repair the problem. Escalations are to be made by the Central Directorate for IT & Communications.
- Access to ECA's systems and hardware by the vendors
- Spare parts provisions including the quantity of critical spares that must be available, who owns the spare parts, and where they are to be stored
- Performance credit calculations when service levels are not met
- Penalties, conditions for invoking penalties, and enforcement
- General Terms and assumptions on systems and infrastructure environments

It is the responsibility of the Procurement unit in Finance and Administrative Affairs to monitor SLA performance. The Help Desk and other organizations within the sector will provide the collection of information and reporting needed for F&AA to perform this monitoring.

2.11 INTERNAL AUDIT

An audit of the Technology Sector should be conducted yearly. Random or unannounced audits should be being conducted for on an ongoing basis specifically for security.

The yearly audit should be conducted by a GoE Central Audit organization working closely with the Standard Operating Procedures and Guidelines unit with the Technology Sector. These organizations typically have their own rules, procedures, and methods for conducting an audit. They should include the following areas in their audit:

- Documented system maintenance procedures
- Documented help desk and problem reporting/tracking procedures
- Backup/recover, and storage of backup media procedures
- Enforcement of service level agreements with system vendors
- Compliance with security awareness and signed security and data confidentiality agreements
- Responsibilities for security and security management are well known and understood within the Sector
- Data, files, transactions, and sensitive information are protected through encryption, passwords, system access and other means
- Compliance with system development lifecycle standards including development standards and documentation standards
- Asset recording and management procedures are being followed
- Project management procedures are being followed for all major projects

The random or unscheduled security audits may be conducted by a GoE Central Audit organization, with assistance from another government IT Audit group or a firm or entity outside of the GoE that has IT audit skills. The areas of concentration should be on following written procedures and compliance for:

- Password issuance and controls
- Access rights and privileges to systems
- Physical access and asset protection controls within the data centers
- Storage and security of system backup tapes including offsite storage
- Internet Usage
- Antivirus updates
- Security awareness
- Configuration control and software distribution/update procedures
- Asset management

2.12 CLIENT SATISFACTION

Client satisfaction is very important to the Technology Sector. Client satisfaction goals and measurements will be defined and implemented.

The client satisfaction goals are to achieve a “4” satisfaction level by the end of year 2, of the average across all responding users, on a scale of 1 to 5, with 5 being a completely satisfied. The key items to be measured in the client satisfaction survey should tie directly back to the key performance indicators defined by the Sector, as discussed in a previous subsection.

Satisfaction is based on questions of timeliness of processing and delivering results; quality of the data and results; responsiveness and ability of IT to meet new demands, ability of end-users to contact IT and have problems resolved and whether feedback during problem resolution is sufficient; and whether the user perceives value in what is being provided by the Sector.

A satisfaction plan will be developed by the Technology Sector. It will include:

- Objectives and goals. The primary goal of the satisfaction plan should be to improve overall Technology Sector delivery of services to its clients.
- Confidentiality of participants and individual results. The confidentiality of each individual participant must be protected, and assurances given that the participant survey results will remain confidential under any and all circumstances. If confidentiality cannot be assured, the participants' results may be skewed ignoring or not providing good data on real problems. And issues.
- How to conduct the survey. The survey may be done online or via a paper document. Online is preferred, but confidentiality must be assured.
- Survey contents. The survey should be short, no more than 12 questions. It should ask for the participant's evaluation on:
 - Value of services provided
 - Value of support provided
 - Ability to deliver services and support within reasonable timeframes
 - Time to repair, fix, or respond to a problem or request
 - Did the support organization understand the problem; was the real problem correctly understood and fixed, or was some of the problem worked on.
 - Did the support organization keep the client continuously informed of the progress in resolving the problem, delivering the service, or answering the request.
 - Did the support organization keep the client informed accurately of when the problem would be resolved, the service delivered, or the request answered.
 - Identify the participants
 - How easy and convenient is it to contact the Help Desk
 - Did the problem get resolved
 - What is your value of the overall support organization to you in terms of doing your job
- Identify Participants. A statistically significant sample or all end users of the system. A % of participants in each category of end users should be selected. The total number within each category should be sufficient so consolidated results within any category will ensure confidentiality of individuals.
- Conduct the survey. This should be done annually.
- Data collection and analysis. The sector should consolidate answers within end-user categories (internal, external, government, non-government) and average the results. Statistical techniques include using standard deviations, means, and medians may be used. It is best to keep the analysis simple, typically by simply averaging the results of each answer within a category of users.
- Comparison of analyzed data with benchmarks established in the goal setting. The goals should be to show improvement in the same survey question from year to year, and to demonstrate general improvement across the entire range of questions. Client satisfaction results will be analyzed with emphasis given to comparisons between years to detect ongoing and new problem areas.
- Identify issues and obtain management concurrence on priorities. Those averages that either fall below a "3", or are less than the previous year's score need to be highlighted for further analysis and then prioritized. The results will be given to the Director Technology Sector. The results should include an explanation, whether good or bad of why the score for a survey question has fallen, but, without providing excuses and minimizing the impact of the problem. Management of the Sector and the IT Governance Board should review the results and concur on the problems to be addressed and the priorities.
- Develop plan to address issues. All problems and issues with high priorities need to have an action plan developed that addresses specifically how to resolve the problem and increase the client satisfaction for particular problem.
- Execute the plan and resolve high priority issues. This is an ongoing activity to be performed by the Technology Sector throughout the year.

Client satisfaction results should be used in employee annual evaluations where direct linkages can be established between reported client satisfaction and goals established by IT personnel in their annual performance plan.

2.13 SECURITY

Information systems security is critical to the organization's survival. Security Policy and Procedures require special attention because these protect the organization's information assets from threats.

The responsibility for security at the time of this draft is not assigned to any unit within the Sector. Instead, security is everyone's responsibility. It is expected that in the future a single person or unit within the Sector will have overall responsibility for security policies, procedures, and enforcement.

It is the policy of the Sector to ensure that:

- Information will be protected against unauthorized access
- Each employee of the ECA understands that it is their responsibility to protect information system resources within their control and possession or to which they have access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Personnel security requirements will be met
- Physical, logical, and environmental security (including communications security) will be maintained
- Legal, regulatory, and contractual requirements will be met
- Information security awareness training will be provided to all staff
- All breaches of information systems security, actual or suspected, will be reported to, and promptly investigated by Legal Affairs
- Violations of Information Security Policy will result in penalties or up to and including termination of employment

All managers are responsible for implementing information security policy within their area of responsibility. Each ECA employee is responsible for the security and protection of electronic information resources over which he or she has usage or control. Resources to be protected include: networks, computers, software, data, and facilities. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. These same protection requirements apply to all clients of ECA using ECA resources.

It is the policy of the Technology Sector to provide layers of security within an overall framework. These include both electronic, systems, and physical security. The Sector recognizes that security breaches, violations, and intrusions can occur from numerous areas within and external to the ECA IT systems, hence a layered, multiple protection policy is required.

In support of this layered approach, security policies will be presented in the following areas:

- Data Confidentiality
- Data and network encryption
- Password and system access controls
- Transmission and transporting of data and files
- Remote access
- Internet Usage
- Personal computer usage
- Software updates
- Antivirus

- Firewalls, intrusion prevention/detection
- System logs and recording of activities
- Reporting of violations
- Enforcement and penalties

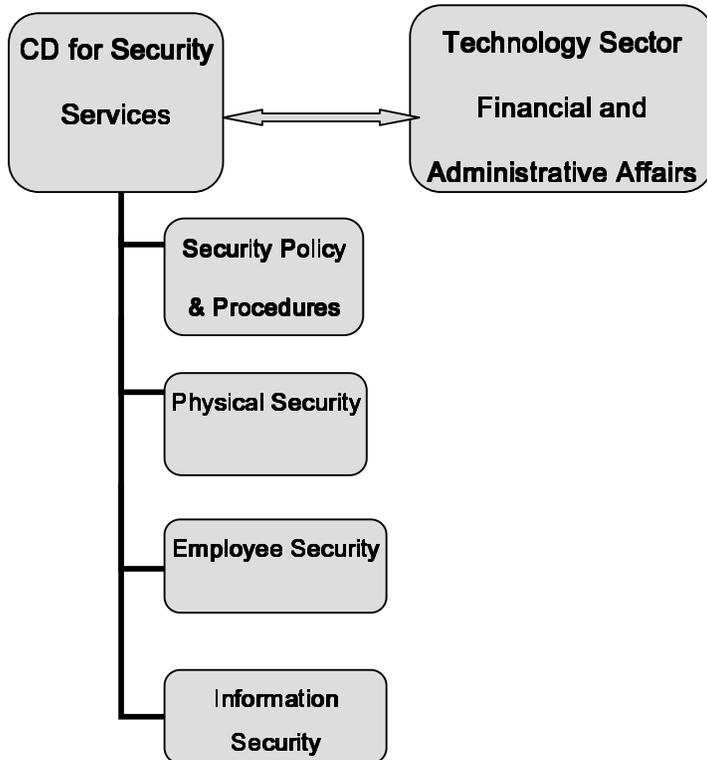
It is the policy of the Technology Sector to recognize that data has different classes or priorities for confidentiality that results in different security needs. The classification takes into consideration the potential damage to the ECA and the government if confidentiality is breached. Three levels of confidentiality will assigned to data:

- Highly confidential whose unauthorized use would cause political and operational damage to the ECA and potentially to the GOE. This data requires the greatest degree of security including encryption, very restricted access, and system logs to record all changes. Examples of this are: Customs client's identification number and financial records; human resources information; and passwords. This type of information and the systems in which it resides must have access controls that ensure the data residing in these systems is not disclosed, modified, deleted, or made unavailable in an unauthorized manner.
- Confidential whose unauthorized use potentially would cause damage to the ECA and/or the GOE. This data requires security measures that have reasonable assurance that this data is not being accessed by unauthorized personnel and has reasonable measures in place to protect its integrity. Examples of this data are: ECA reports, internal statistics, and consolidated information from client data where the source may be derived or inferred.
- Customs data, but not considered confidential. This is commonly public information that carries no liabilities if it is shared or transmitted outside the ECA. Data of this type can be shared within the ECA without access controls. Integrity rules are set up by the users.

It is a violation of Sector policy for users to attempt to gain unauthorized access to any electronic information or to alter, damage, or disrupt the operations in any way.

Technology Sector will coordinate its efforts and obtain approvals, guidance, and direction from the Central Directorate for Security Services as shown in the following diagram.

Coordination of Technology Sector with Central Directorate for Security Services



- Coordination of Technology Sector and CD for Security Services**
- **Policies and Procedures**
 - **Enforcement and Penalties**
 - **Personal Computer and Systems Usage**
 - **Data Confidentiality**
 - **Internet Usage**

2.13.1 Data Confidentiality

Sector policy requires all employees to sign a data confidentiality agreement. Appendix A contains a detailed example of such an agreement. Employees agree to protect all data within all ECA systems, to not send this data to any unauthorized person, to not exploit this data for personal use, and to abide by other policies regarding maintaining data confidentiality. Breach of this agreement may result in termination of employment and in severe breaches criminal prosecution.

2.13.2 Data and Network Security and Encryption

The Sector policy requires that any network used by the ECA must ensure that data transmitted in the network is secure from outside unauthorized access. Private networks, those dedicated solely to the ECA provide this protection. Other connections that operate on public rather than private networks expose the ECA to the possibility of data theft. Any non-private network used by the ECA must provide encryption of at least 128 bit encryption. This will provide data protection by encrypting and decrypting the data as it enters and exits the nodes of the network. This type of encryption is provided through standard routers.

Virtual Private Network (VPN) controlled-access using security tokens and passwords are to be utilized for all system access, by all categories of users.

All access to and connections to the hardware or network components to ECA systems and networks must be approved by the Sector Director of Technology. Access to these networks and systems is to be tightly controlled. New protection devices and software will be added as needed to ensure protection of the network and systems.

2.13.3 Transmission and Transportation of Data and Files

All data and files that are electronically transmitted must be done on secure networks. The networks must be approved by ECA, and demonstrate that they are either private networks, and or provide at least 128 bit encryption of data.

Transportation of data and files on external media between ECA locations must be done only by approved courier. The information is considered confidential, hence it must be protected. An example of transportation of data and files is the movement of database backup tapes from one location to another within the ECA.

All physical data media, leaving or entering a Technology Sector location must be logged and authorized by the IT shift supervisor at that location. The log must include: description of what data was transported; when; who received it and to whom it was to be sent; date and time of receipt/transport; type of media; and disposition upon receipt. This log is to be kept for at least one year in a fireproof safe.

All data received from clients and defined as confidential or requiring security must be physically marked on the package, and electronically marked in the heading information to the data.

2.13.4 Passwords and System Access Controls

2.13.4.1 Roles and Access Privileges

Sector password policy establishes a standard for creating strong passwords, protection of these passwords, and frequency of change. Passwords are the frontline protection for user accounts; as such a poorly designed password system may compromise the entire ECA network. The scope of the policy will include all personnel who have or are responsible for an account on any system that resides at any ECA facility.

Passwords will be issued for all users of the system upon the written request of the person's supervisor and the Head of the CD for IT & Communications stating the specific access rights and which specific systems are to be accessed.

Roles for access rights and privileges will be defined by the Sector Database Administrator and approved by the Director of the Technology Sector. These roles will be used to match access requests for the various types of users.

An encrypted database will be established and updated for all access roles, access privileges, individual accounts, and passwords. This database should reside on a hard disk separate from the main system's operating system and operational databases. It is to be accessed only by the database administrator and the Director of IT & Communications. This database is to be backed up each night, and separately from all other databases. It is to be stored in a locked safe.

System administrators have a higher more secure access to the systems because of their need to assign and monitor passwords of all other users.

ECA management and/or the Human Relations department must notify IT Sector on the hiring of or dismissal of employees so that the access rights and privileges can be initiated or revoked. In the event of a planned employee dismissal this notification must take place prior to the employee's being notified of his or her dismissal so that all access rights and privileges can immediately be revoked.

2.13.4.2 Passwords

It is the policy of the Sector that passwords are to be changed regularly, are not to be shared, and are to be secure.

Mandatory changes to passwords will be required at least every four months. The prior 6 passwords will not be accepted. Passwords must be at least 8 characters in length, and must contain at least 3 out of the 4 following character types: digits, alphanumeric, special characters, capitalized character. The new password must have at least 50% different characters than the previous password. Passwords cannot contain any portion of the person's name(s).

The system will deny access to any user who does not change passwords when notified by the system, or who fails to provide a new password following the create/change rules. The "locked" out person will be contacted by his/her manager to resolve the issue.

System administrator passwords should follow the same general rules as other passwords. Since they allow access directly into the secure password files, the system administrator passwords should never be written down, shared, or displayed on a computer monitor. System administrator passwords must

be changed at least every 90 days. The Director for IT & Communications will be responsible for enforcement of these procedures

Passwords are not to be included in email messages. They may be transmitted in an encrypted attachment or via telephone.

Users of the ECA systems are not to provide or share their password information with anyone, either inside or outside of the ECA. Passwords are considered privileged and confidential information.

Employees found to have violated password security may be subject to disciplinary action, including denial of access to system resource, and up to and including termination of employment.

2.13.4.3 Authentication

Sector policy requires all system users will be verified via VPN/AAA authentication and authorization using a series of logon ID's, passwords, and token or other dynamic ID's. Tokens and other physical devices will be issued, inventoried, and managed by the Technical Support department.

2.13.5 Remote Access

Customs employees may access the system remotely through approved procedures and only for official ECA business. The access must use VPN software and remote access secure tokens. Public and private dialup, and Internet connections may be used. Remote access users must get prior approval from the head of IT at their reporting location, as well as the Sector Director Technology.

2.13.6 Internet Usage

Sector policy requires that any ECA employee requiring Internet access, may access the Internet through ECA computing resources and only through ECA approved networks. These networks or channels are the ones defined, provided for and used by the ECA. Internet access is not to be obtained through unauthorized dial up connections, or through the use of ECA Internet connections using non-ECA computers. The channels for access must utilize standard configurations for firewalls and/or proxy servers and be managed centrally.

Internet usage is limited to business purposes only. Technology employees are not to access non-business related websites except in the course of performing their jobs.

Internet information may be downloaded and stored on ECA personal computers, as long as it is related to ECA business and is utilized in the performance of an ECA employee's job.

2.13.7 Personal Computer Usage

Personal computers are to be used only and solely for ECA activities, work, and, tasks. No personal use of application systems, document management, word processing, spreadsheets, graphics, and the Internet is allowed.

Loading personal or any non-ECA software, files, games, pictures, etc., onto ECA personal computers is prohibited, unless the Head of IT at that location and the Sector Director authorizes the request in writing.

Laptop personal computers are to be used only for ECA activities, work, and tasks. They are not to be used by anyone outside of the ECA. Laptops must be locked and stored in a secure area when not in use outside of the ECA facilities.

2.13.8 Software Updates

It is the policy of the Sector that all system and database software provided by vendors will be kept current through multi-year software upgrades maintenance agreements. This is especially important for those portions of the system that provide security protection such as antivirus, intrusion detection/prevention, firewalls, routers, and other system components or appliances.

Security updates to software will be made as received from the vendors. Other software version updates will be analyzed for their impact on users and then schedule as a version update for implementation.

Software updates will be applied using the system maintenance and update procedures and under the guidance of quality assurance.

2.13.9 Antivirus

It is Sector policy to use one and only one enterprise antivirus software package. ECA should enter into a multi-year software upgrade agreement with the antivirus software vendor to ensure that they receive the latest software updates.

The antivirus software will be administered and controlled from the primary data center, with updates received each day from the vendor to the antivirus control server. These updates are then to be electronically transmitted by the Technology Sector to all remote locations.

All PC's are to use the ECA standard antivirus software. The PC's are to be configured so that at least once a week, upon powering up, they automatically receive all antivirus updates from the server that controls antivirus updates at their or any other location within the ECA. Laptops must be powered up and logged onto the ECA network at least once a week to receive these antivirus updates. The PC's should be configured so that these weekly antivirus software updates cannot be bypassed.

Procedures require that any file or macro attached to an email from an unknown, suspicious or untrustworthy source should never be opened. These emails should be reported to the IT manager at that site for proper disposition.

2.13.10 Firewalls and Intrusion Prevention/Detection

Any location within ECA that has a link to the "outside" world on the Internet or other connectivity must have a firewall to protect itself against unauthorized entry. Threats and risks change daily, so it is the policy of the ECA to keep these firewall and other appliances updated with current software. This requires that the IT Sector enter into multi-year software upgrades for these devices.

Demilitarized zones will be installed at each sites that have Internet/Extranet access by using firewalls and edge routers.

2.13.11 System Logs

All ECA systems that have the network operating system and/or the database management system (DBMS) must log certain types of system requests and events and maintain audit trails. This logging will provide history that can be used, interrogated, and analyzed for security breaches.

The facilities within the operating system and the DBMS should be invoked so that all logons, password changes, access privilege changes, and denials of accesses are recorded in the log files. These files are to be backed up every night, stored in a fireproof safe, and kept for at least 1 year.

2.13.12 Reporting Violations

All ECA employers are required to promptly report security violations to their immediate manager. This applies to observed violations and to knowledge of others who have been misusing the systems. Violations are then to be reported to the Sector Director. Detection of violations and improvement in security procedures can only be accomplished if all employees understand their responsibility in reporting violations.

2.13.13 Enforcement and Penalties

Enforcement is the job of all Technology Sector employees. Overall enforcement responsibility is with the Head of IT at each location. The Head must distribute the Data Confidentiality Agreement yearly, and discuss with his/her employees the policies and procedures for enforcement and penalties.

Serious breaches of security such as the unauthorized removal of confidential data, and providing this data to someone outside the ECA may result in loss of employment. These are serious violations and simply issuing a warning to the offender is not sufficient. These violations should be reported to the Head of Legal Affairs at that location for possible criminal prosecution.

Other violations of a less serious nature include: failure to lock confidential data in a safe; failure to transport a backup tape to an offsite location; failure to change a password. These should be dealt with on an individual basis with specific penalties depending on the history of violations of that employee. As a guideline, no more than 3 violations in any one year should be allowed without consideration given to serious penalties including dismissal of the employee. Continuing violations over a period of time, beyond one year should be considered during the employee's annual appraisal, and may result in reducing the employees rating and potential pay increase and bonus.

Technicians at the main processing centers need to monitor the system and event recording logs on a daily basis to ensure that the system is not being attacked or subject to some malicious entry. Technicians will receive specialized training in the system software that allows them to monitor, detect and take corrective actions.

All firewall, router IOS, intrusion prevention or detection, and operating system access and event recording logs must be maintained and backed up along with the databases each day. These access and event recording logs are to be analyzed monthly by the Technology Sector to find potential system access or attempted access violations. One reason for keeping 4 weeks of daily, 12 months of monthly, and a yearly backup tape is to have historical data available for specific searches for a violation, and to be able to do longer-term audit and analysis.

2.14 BUSINESS CONTINUITY

Business continuity is the process of planning, executing, and protecting the ECA's computer facilities from a major or less serious interruption. Business continuity and its shorter-term counterpart as it relates to the Technology Sector, backup/recovery, consists of the following areas of policy and procedures:

- Disaster Planning and Redundancy
- Backup/Recovery
- Physical Planning and Protection
- Disaster Recovery Training

It is the policy of the Technology Sector critical IT processing services will be out of service for no more than 2 consecutive hours.

2.14.1 Disaster Planning and Redundancy

In the new Technology Sector structure there will be at least two major processing centers, at Alexandria and Cairo and optionally at a 3rd location. These should be configured so that they are capable of fully backing each other up in the case of either a short or a long duration of system unavailability. The hardware, network, and software configurations are to be similar, and to provide sufficient excess capacity to take over the entire processing of the site that is lost for a period of 6 months.

User services should be classified in terms of priority or criticality. Not all services are needed immediately when the system is lost for extended time periods (e.g., several days). The critical services are: processing of core functions such as manifest entry, declaration processing, online bank payments, exchange of information with GOIEC, Trade web services, and cargo tracking. These are the services that require almost immediate backup at the disaster planning backup center when the main site is out of service. These critical services must not experience an outage for longer than 2 hours. Other services such as reports, non-time critical data entry, producing reports, and processing done on a time cycle longer than 3 days do not have to be back in service immediately. These services will eventually be made available, but only after the critical services are fully restored.

A plan should be developed that provides the details of exactly how this transfer of the entire processing of one data center to the other will occur. Disaster planning includes more than the IT related tasks; it must include those core functions to be performed by end-users. The specific tasks, personnel responsible, the expected timeframe for performing the task, how the service or function will be restarted, how key personnel will be contacted and how they will report to the backup location, and the various dependencies all need to be defined in this plan. The plan should specify emergency response procedures, including specifying personnel assigned responsibility for responding in emergency situations, procedures to enable team members to communicate with each other and with management during an emergency, where emergency personnel are to report, and what resources are to be moved or reinstalled at the disaster recover site. End-user management must be engaged in defining their critical personnel and how they will be activated, moved to, and managed at the backup site in the event of a prolonged system outage or other loss of key system resources.

This detailed plan needs to be fully tested and implemented at least once a year to ensure that those responsible for its execution are capable of performing the transfer of processing, and that the procedures described work successfully.

The risks that may cause the plan to be invoked need to be identified, the resulting expected damage quantified, and prioritized. These include: earthquake, fire, water damage, terrorist attack, loss of network, and loss of key operating personnel.

It is the policy of the Sector to design redundancy in its systems in order to provide 100% failsafe operation on critical system components, 24 hours a day, 7 days a week. Major centers must have “hot” backup to another center. WAN’s must have backup of critical core routers, switches, firewalls, network links, and instant switchover to the recovery system. Critical devices such as servers, core routers and switches, must have dual power supplies. UPS’s will provide at least 15 minutes of system up time for servers and other critical system components.

2.14.2 Backup/Recovery

It is the policy of the Technology Sector to maintain multiple backups and to have backups stored at both onsite and offsite locations. Backups of all databases are to be made once a day (night). The procedures to be used are:

- These backups are to be made to tape or other removable media
- Tape or other removable media is to be stored onsite in a secure safe protected from water and fire damage
- Tapes are to be made daily and kept for a period of 28 days.
- Backup media must be clearly labeled with Day 1, Day 2,,,,,Day 28 so that the same tape can be used on the same day in the next 28 day cycle.
- All tapes in a 28 day cycle must be continuously accounted for.
- The twenty-eighth day tapes are to be kept for one year.
- Year end tapes of the system are to be created.
- Tapes are to be clearly marked with date created, by whom, shift supervisor’s signature, databases backed up and from which server, and which volume for multi-volume backups.
- A duplicate tape is to be created, transported to another location within the ECA and stored in a safe protected from water and fire damage. Two locations can transport their daily tapes back and forth on a daily basis to each other for this purpose.
- Where possible, system automated and scheduled backups are to be performed.
- Full system backups and duplicates are to be made every week. This will include application runtime libraries, configurations, etc. These are to be stored for 56 days (8 weeks).
- Specialized backups for system logs and system access/privilege databases must be done to separate tapes.
- Technology Sector shift supervisors are to ensure these procedures are followed and sign off on the procedures, that the tapes or other media have been created daily, that they have been stored, and that the duplicated copies have been transported to another location.
- Recovery of both databases and the full systems images are to be tested every 3 months to ensure that the restores can be successfully performed.
- Old backup media, older than 28 days can be reused for the next cycle.
- The two main centers will mirror their databases so that each center will have a complete replication of the other’s databases.

All servers and PC’s should have a UPS backup device available, one that will provide at least 15 minutes of up time for servers and other critical system devices; and 5 minutes of up time for PC’s at full power in event of loss of the main electrical supply.

2.14.3 Physical Planning and Protection

It is the policy of the Sector that facilities that contain confidential information be secure at all times and that measures be taken to prevent unauthorized persons from gaining access to these facilities.

All data processing centers will have locked doors at their entrance. A list of authorized personnel will be maintained by the operations manager. Personnel not on that list will be required to sign in and be authorized by the shift operations manager. All personnel are required to sign in and out of the computing data centers. This daily log will be maintained in a fireproof safe for 1 year.

All data processing centers will have adequate fire protection, smoke detectors, heat detectors, and fire extinguishers. They will have adequate air conditioning, electrical power, power stabilization and regulation, backup electrical power via a generator, and UPS's to protect the entire center. In areas where air-borne particulate (e.g., dust) is a problem, enclosed equipment racks with air filtering mechanisms are to be used.

Data center personnel will be trained on how to operate fire extinguishers. They will be trained on what ECA procedures are to be followed in the event of a fire, earthquake or other damaging or catastrophic event, including whom to contact and how to contact key personnel. These procedures should be posted in a prominent place in the data center.

Server systems should be available 24 hours a day, even during times when they are unattended, in support of the objective of offering 24 hour service to certain categories of clients. Server rooms are to be locked during hours when Technology Sector personnel are not in these rooms.

Servers should be locked out when not being attended; e.g., they require a systems administrator login to regain access.

All PC's should be locked when not in use for more than 30 minutes. This requires the user to enter an ID and password to re-login.

ECA management must immediately notify the IT manager of system access rights when an employee is terminated.

2.14.4 Disaster Recovery Training

Technology Sector will conduct an annual Disaster Recovery training seminar for all of its employees. This may be combined with the annual seminars on security policies, procedures and the Data Confidentiality Agreement review.

2.15 EMAIL SYSTEM

It is the policy of the Sector to have single, and standard email system in the ECA. The use of free email systems such as Hotmail and Yahoo will be eliminated as the new standard email system becomes available. Use of an unauthorized email system is prohibited and may result in penalties.

Email usage is restricted to the conduct of and support of business by the ECA. Use of emails for solicitations and personal business is prohibited. Guidelines on the use of email will be part of the annual Security Awareness seminar provided to all Technology Sector employees.

2.16 ASSET MANAGEMENT

The Technology Sector has a policy for managing its assets. It will utilize standard operating environments (SOE) at all IT locations.

2.16.1 Asset Management

All IT assets will be recorded and maintained in an electronic database. When new equipment is received its serial number, brand, model, vendor received from, cost, maintenance provider, date received and warranty period will be recorded. Its location is to be recorded, including whether in storage, in a production site, at a vendor for repair, or other. When an asset is removed temporarily for repair or permanently at the end of its life, the date, reason for removable, and where the asset is being transferred to will be recorded. A label will be created and applied to the asset that shows date installed and the vendor it was procured from, the maintenance provider and how to contact the maintenance provider.

Assets will be grouped by type, such as desktop PC's, laptops, black and white laser printers, color laser printers, matrix printers, scanners, servers, routers, switches, hubs, security appliances, racks, UPS's, etc.

Standard software configurations and images will be maintained for all desktop PC's and laptops. These will be controlled through the system configuration control software on the servers at the main processing centers. These configurations and images are not to be altered at any location. Updates to software will be sent to the locations electronically and then applied to each desktop PC or laptop. The configuration control systems and the asset management system will be updated to show what software is installed on each desktop PC and laptop.

All movement of computer equipment must be recorded in an electronic Asset Recording and Tracking System (ARTS). The movement from an area is recorded independently from the move into an area. Shift supervisor signatures are required for all moves out of or into an area.

2.16.2 Standard Operating Environment

It is the policy of the Technology Sector to utilize standard operating environments (SOEs) to the maximum extent possible. The purpose of this is to lower maintenance costs, reduce operational problems, and increase worker productivity by minimizing the number of differences between the same general type of equipment. SOEs will be defined for servers, PC's, laptops, laser and matrix printers, tape backup devices, disk storage devices, switches, routers, firewalls, and security appliances.

Standard operating environments will be maintained for each piece of equipment by recording the SOE and configuration in the Asset Management system. These will be maintained by the Infrastructure Department.

New procurements should use existing SOEs as a guideline. At the time procurement requirements are being developed, SOEs may be updated as a result of advances in technology.

The standard operating environments, especially for servers and PC's will change as technology improves and as costs become lower. Older SOEs will remain compatible with the succeeding ones for at least 3 years.

The SOEs for PC's should specify: memory size, processor speed, hard disk type and capacity, floppy disk, CD/DVD, USB ports, NIC card, monitor type and size, operating system, office suite software, and primary Customs and non-Customs application software resident on the PC.

Servers will come in several classes depending on the type of work they process, their complexity and their capacity. These can be defined as large, medium and small servers, with additional qualifications based on application or database servers; network or security servers, file or reporting servers, and other specialized servers. The types of servers, which will fall into these estimated 4 classes include: Database server, application server, web server, workflow server, data warehouse server, reporting server, email server, domain/controller server, firewall server, authentication/authorization server, file server, network server, and others. The server specifications depending on class are: memory size; number of processors, type and speed; number of hard disks, type, hot plug, capacity, and speed; tape backup device, type, capacity and speed; RAID type; rack or floor mounted; level 2 and 3 cache; redundant power supply and fans; NIC interface cards, types and number; multi-channels; operating system; tape backup software; CD/DVD; USB ports; floppy disk drive.

Printers should specify: model; type (laser, inkjet, matrix, impact); maximum page size; normal print speed; monthly rated capacity; number of input trays, memory size; optical resolution; network or USB connectivity.

Data storage devices should specify: model; type (SCSI, SATA, SAN, NAS, etc.); number of disks or containers; storage capacity, type of physical connectivity; number of connectivity ports, interfaces or adapters.

Network devices should specify: model; type; number of ports and speed of each port; type of port connections (fiber, Ethernet, etc.); DRAM memory; Flash memory; auto-sensing; image type; interface types.

2.17 DEVELOPMENT STANDARDS

The Sector recognizes that development standards will largely result from the choices made for vendor software. Where reasonable and feasible, the number of development standards should be kept to a minimum; i.e., the software suites utilized should be the same or at the very least compatible for among the various vendors. This will reduce maintenance costs, the need for additional skills within the Sector, and IT technical training.

2.17.1 General Standards

The Sector will utilize international standards as provided by the software vendors for the major application processing system. These standards will evolve over time, but they at a minimum include:

- XML
- Relational databases such as Sybase or Oracle or MS SQL Server
- Development tools and suites of Java or .NET or PowerBuilder

- Configuration and version control software
- Report writers (e.g., continue to use PowerBuilder, or Crystal Reports)

2.17.2 Development Lifecycle

A system development lifecycle methodology is to be used for all new systems development and major enhancements to existing systems. These procedures are to be followed whether the development is done by the Technology Sector or by a vendor. In the case of vendor development, the Sector's role is to participate fully in all phases and to emphasis management of the plan and the deliverables. The development stages should include and use the following:

- **Planning** – establishes project plans and management reporting and controls for a specific project. Standard project planning tools such as Microsoft Project should be utilized. The plan should include major phases, tasks, resources assigned, timeframes, milestones, deliverables, identifiable risks and how to mitigate these, change control, approval procedures, project communication, and standards to be employed on the project. Planning includes the procurement of software and hardware, and specifying and setting up the development and test environments.
- **Requirements** - consists of a statement of the business, functional, security, and performance requirements, the business problem to be resolved and the potential solutions.
- **Analysis** - consists of an analysis of alternatives, cost/benefit analysis, buy versus build analysis, and a statement of the preferred system solution.
- **High Level Design** – consists of forms descriptions, report descriptions, Entity/Relation diagrams, data flow diagrams, test considerations, system architecture, and data model. Users should review the requirements with the designers to identify the missing functionality. Designers propose a solution with the rough estimate of time and cost. Users and technical staff review the design and approve.
- **Detailed Design** – consists of detailed forms, logic, report logic, cases and instances, concurrent programming logic, database design, integration issues, unit test cases, installation instructions. Users and technical staff review the design and approve. Cost and time estimates from the previous phases are updated. Coding quality is to be checked by using at least one test case for each requirement. Scheduled reviews are to be made with users after the solution is documented, the detailed descriptions are completed, and the total design package is completed.
- **Build and Test** – consists of code customization, test, installation to demonstrate functionality, and testing with the users to verify the functionality.
- **Deploy** – consists producing final documentation, turning the production code over to the technical support staff, site preparations, user training, and installation of the system in a production environment.
- **Operate** – consists of ongoing operations, support, measurement of, and gathering and analysis of new requirements and enhancements to the system.

2.17.3 Development Guidelines

Development guidelines will be defined by the vendors providing major systems and/or by the Technology Sector. Quality Assurance will define the Sector guidelines and work closely with vendors to ensure that the following guidelines are adhered to. Vendor software may not be flexible enough to allow the Sector's guidelines to be followed. In those instances Quality Assurance should develop modified guidelines to minimize the differences between the vendor's and the Sectors guidelines. The guidelines apply to:

- Naming conventions
- Directory naming conventions
- Object definitions

- Development techniques
- Coding standards should address standards for database objects; table standards; views; package procedures, triggers, and functions; database schemas, date formats, programming standards, cursor definitions, exception handling, error handling, custom forms, custom report.
- Commenting within modules is encouraged and should be dated if the version control software does not supply this.
- Design reviews
- Exception and error handling
- Source code control and version maintenance
- Migration approach

An approach taken for modifications and program maintenance is needed to produce high quality, consistent look and feel, ease of maintenance, compatibility with future versions of the software, and portability across all platforms. Guidelines for customizations of should be designed to:

- Minimize the impact on core application functionality
- Permit easy upgrades to future releases of software
- Allow customizations to be easily reinstalled
- Insure that customizations meet the users' requirements
- Insure the high quality of delivered code
- Involve users in the final testing
- Facilitate the transfer of responsibility for code maintenance to the Sector through classroom and on-the-job training

Control libraries must be used for all stages of development. Migration from one stage to another should be done using formal procedures and only after testing and management approvals have been made. Migrations are to be performed by the Quality Assurance administrator or the DBA.

Only servers are to be used for storing software in any of its development stages (design, prototype, pilot, pre-production, test, production). These software repositories on servers are to be the sole source of all software at any stage in its development, testing, maintenance, and deployment. PC's are not to be used to store copies of software under development or maintenance because of the potential problem of losing control over the versions.

2.18 DOCUMENTATION STANDARDS

Documentation will be produced by software and hardware vendors, and by the Technology Sector. For internally produced documents what is described below will apply. For vendor supplied documentation Technology Sector will ask vendors to conform to the internal standards where possible. Where this cannot be done, Technology Sector will require the vendors to alter their documentation to conform as closely as possible to the Sector's standards, and/or the Sector may customize the vendor's documentation to better fit its internal standards.

The following are the documents that in one form or another should be included in the set of documentation of any major application system. This list is a consolidation of BearingPoint's best practices for Project Software Life Cycle Development, and the Capability Maturity Model's (CMM) Software Development Documentation for Level 2 and 3. A summary of the primary contents of each document is included in the descriptions. Not all of these documents have to be used in all

projects. Some of these can be used for major proposed changes to existing systems, while new and large projects should include most if not all the documents in the following list.

1. General Documentation Standards (applies to all subsequent documents)
 - Describe purpose and target audience
 - Describe version controls and rules on how to maintain the set of documentation
 - Describe the organization and basic content of each document in the standard set.
2. Project Plan
 - Describe the overall project plan including management structure, and project organization.
 - Define communications and project reporting structure.
 - Define project management approach, roles, and responsibilities.
 - Define project risks and management and mitigation of risks.
 - Define basic baseline project plan with phases, tasks, resources and skills required, timelines, milestones, and deliverables.
 - Define plans for change control, training, quality assurance, audits and reviews.
3. System Requirements Specification
 - Describe the objectives, general description, and overview of the system.
 - Define the system owner(s), system pre-requisites, and list of major functions.
 - Define general system requirements and architecture, including network, hardware, volumes, performance, availability, reliability, security, and other system characteristics.
 - Define detailed functional requirements for end-users, administrators, backup/recovery, language support, customization, and security.
 - Describe basic inputs and outputs.
 - Define programming and design standards and standards compliance.
 - Describe Database Management System and logical database requirements.
 - Describe critical dependencies.
 - Define design constraints.
 - Describe interface requirements with other systems, hardware and communications.
4. Software Requirements Specification (often incorporated into the Systems Requirements Specification)
 - Describe software development tools to be used in detail.
 - Detail descriptions using charts, diagrams, and data flows of the functional elements of the system.
 - Quality control requirements including configuration, version, and change controls.
5. Data Base Design
 - Describe all tables, all entities, and characteristics of entities.
 - Describe primary and foreign keys.
 - Describe editing rules for tables and/or fields.
 - Describe add, delete, updating rules for tables and fields.
 - Provide E/R diagrams for entire database.
 - Describe rules for normalization, referential integrity.
6. Detailed Design and Program/Module Design
 - Describe the coding conventions, names, protocols, and standards to be used.
 - Provide logic charts, call sequences, API descriptions, and invoked procedures descriptions.
 - Define objects and classes.

- Describe detailed programming flows, invoking/calling sequences, and parameter lists.
 - Provide error lists and resulting actions.
 - Describe use of report writers.
 - Provide detailed design of all inputs, outputs (screens, reports).
7. Test Plan and Test Approach
- Define testing approach and criteria for success/failure.
 - Define who does testing, on what level of code (module, multi-module, system, functional, etc.)
 - Describe contents of a test case, and controls for reporting test results.
 - Define test and the control environment, libraries of test cases, test system, control over the test system and access controls.
8. User Acceptance and Integration Test Plans
- Define the testing approach and the criteria for success/failure.
 - Define who does testing and what training is provided.
 - Define who has responsibility for managing, scheduling and controlling the UAT systems environment.
 - Describe contents of a test case, procedures for testing, and controls used for reporting results.
 - Define the controlled test environment, libraries of test cases, test systems, control over the test system and access controls.
9. Site Preparation and Installation and Operator Guides
- Describe pre-requisite site preparations prior to installation
 - Describe system elements and how they relate to the installation procedures.
 - Describe installation procedures, sequence of installation, and controls.
 - List of errors and messages, and resulting actions.
 - Describe monitoring, performance, creating backups, restoring the system, diagnosing problems, and corrective actions.
 - Describe the procedures for reporting and tracking errors.
 - Define whom to contact for help with problems.
10. System and Network Design and Administration Guides
- Provide overview of the system components, hardware, and networks.
 - Architecture chart of the system and networks
 - Define protocols and schema.
 - Define procedures on maintaining inventory of all equipment.
 - Describe details of physical locations of equipment in all locations.
 - Provide wiring, LAN, and WAN diagrams.
 - Define instructions for installation equipment and making network connections.
 - Define configurations of all network equipment, and how to restore these configurations.
 - Define how to add new equipment to the system and the network.
 - Describe directory services, classes of users, granting of privileges and rights.
 - Describe error conditions and resolution.
 - Define and describe problem reporting and tracking of errors.
11. Training Plan and Materials
- Describe training approach (train the trainers, external sources, etc.)
 - Describe organizations that need training and the plan for plan for skills assessment.
 - Describe courses to be provided, timeframe and personnel.

- Describe standard contents of training materials.
 - Describe responsibility for and plan for updating training materials.
 - Provide examples of training materials.
12. End-User Guides
- Define business processes and describe how the system fulfills the needs of these processes.
 - Breakdown of the process into the end-user procedures.
 - Pre-requisite functional and computer skills and knowledge needed.
 - Describe inputs and outputs used for each procedure with examples and descriptions of computer screens and printed reports.
 - Describe error conditions, system messages and resulting actions.
 - System sign-on, sign-off and security procedures.
 - Describe how to obtain assistance, report a problem, and what to do if the system is not responding as expected.
13. Support and Change Control
- Describe Help Desk or other support procedures.
 - Describe problem reporting, tracking and resolution.
 - Describe procedure for formally requesting a system change, including recording of the request, evaluation, cost/justification, and criteria for acceptance or rejection, and notification to the requester.
 - Define backup, recovery, and disaster recovery procedures.
 - Define procedure and checklist for incorporating changes to programs (unit test, user test, documentation updated, update training materials, notify end-users, move from test production, etc).

2.19 TESTING AND PROCEDURES

Technology Sector recognizes that testing for new systems, major system enhancements, and system changes be done using formal procedures. Major projects will require that a Test Strategy document be developed by Technology Sector or the software vendor.

Thorough testing is required with supporting documentation for all types of testing before any programs can go into production. Since vendors will be responsible for most of the future core systems development, Technology Sector must be involved with the vendor in the testing of these software systems.

2.19.1 Testing Types

Five Test Types for software may be used:

1. Unit test – This testing is of individual units or modules of code. This testing is typically performed by the developer who verifies that their piece of code achieves its expected outcomes.
2. Multi-unit or integration testing – This is testing in which software modules, hardware modules, or both are combined and tested to evaluate the interaction between them. This may be referred to as integration testing.
3. Systems test - Systems testing is conducted on a complete, integrated system to evaluate the system compliance with its specified requirements.

4. Performance test – Performance testing validates expected performance of a system, or determines performance limitations of a system. The goal of performance testing is to verify performance requirements have been achieved.
5. User Acceptance or Acceptance test – This is formal testing to determine if a system satisfies its acceptance criteria and are typically based on business requirements. The acceptance criteria enable the ECA to determine whether to accept the system.

A further style of testing that may occur in any of the above five types is regression testing. Regression testing should be performed after making a change or repair of software. Its purpose is to determine if the change has regressed other aspects of the software, i.e., created unintended problems elsewhere in what is being tested. As a general rule, the changed or new software unit should be unit tested and then be integrated into the product and test cases that address potentially impacted areas.

2.19.2 Test Strategy

A test strategy for major software development is required. It should contain most or all of the following:

- General statement of the testing approach, plan and expectations.
- Describe how the testing will be managed, how cases will be assigned, reported, tracked, problem and defect reporting, and how problems and defects are to be prioritized and resolved.
- Test stages to be used and for each the degree of test automation; criteria for success and failure at each stage of testing; testing constraints and assumptions; risk mitigation; and test case management.
- Test types included, such as unit, multi-module, systems, performance, and acceptance testing.
- Types of test cases and expected results.
- Define what is to be tested and what constitutes pass or failure. This may include: code and programs; documentation; procedures for failover and recovery; data migration and conversion procedures; interfaces; installation procedures; system installation and configuration procedures; functional testing; performance testing; security and access procedures; volume testing; regression testing.
- Identify, acquire and install the separate test environment to support each level of testing.
- Identify where testing, especially User Acceptance Testing, is to take place and that there is an adequate facility for testing.
- Define requirements or skills for selecting testing personnel, training required, the role of testers at each level, and who will perform the testing.
- Develop initial test schedule.

No module, program or system will be moved into the production environment unless it has been demonstrated that it has successfully passed unit, systems, and acceptance tests, with signed approvals of the outcomes by the project manager. The testing will be formally conducted by Technology Sector personnel, software vendors, and end-users.

Training is a critical element of preparing for testing. Technology Sector will be provided training by vendors, and both Technology Sector and vendors will provide training to end users prior to testing.

Production data is not to be used for any testing without the written permission of the Commissioner of the ECA. Production data is considered confidential. Production data may be sanitized through combining or “blurring” specific identifiers of the data such as Tax ID, Customs ID, national ID, customer specific financial information, etc.

Customs production data is not to be given to any outside development organization for test purposes without the written approval of the Commissioner of Customs. A detailed description of this data,

numbers of records, and a plan to ensure that the original data is returned and no partial or complete copies have been made, must be included in this request for written approval.

It is the policy of Technology Sector that end-users be responsible for functional testing and acceptance testing. They will be trained in the systems to be tested, and provided guidance and management by the Sector during the testing.

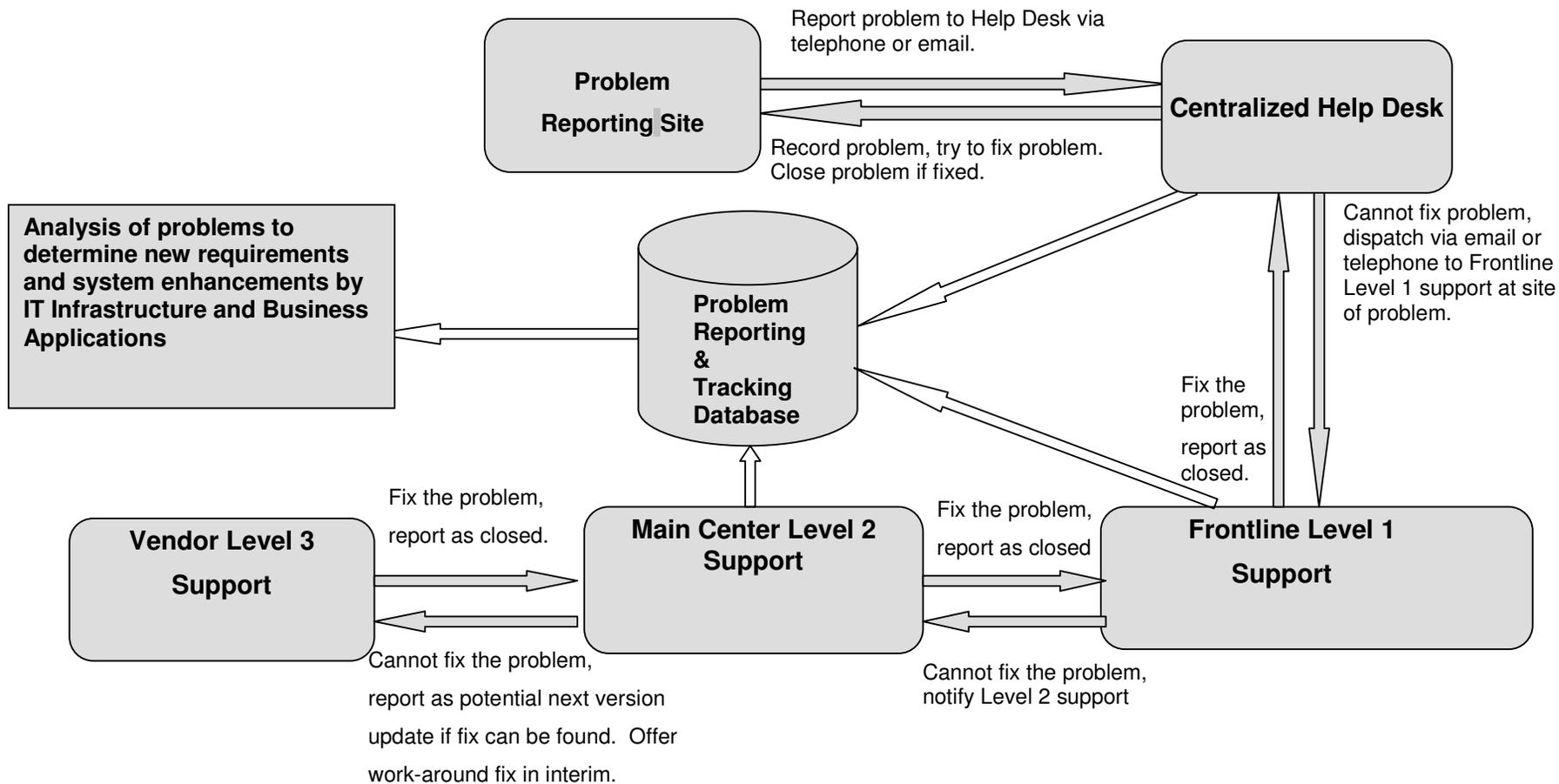
The natural synergy between testing, problem reporting and system enhancements is well understood by Technology Sector. The problem reporting system used for testing must link with the procedure for defining enhancements. The problem reporting system used by the Help Desk must link back to this same procedure and also to the testing of a problem fix.

2.20 SUPPORT

It is the policy of the Sector to be responsive to reported problems, to fix directly or engage maintenance vendors to fix these problems expeditiously, and to use reported problems as a source of future system enhancements.

The first level of support is provided by the Help Desk. All problems are to be called into or emailed to the central Help Desk. This facility will be online, available, 3 shifts 7 days per week. The Help Desk will try to fix the problem. If they cannot fix the problem it will be routed to the Frontline personnel in the facility originating the problem call.

The Frontline support personnel will either fix the problem or call 2nd line support at one of the major data processing centers. If the 2nd line cannot fix the problem, they will call the vendor or maintenance provider to fix or repair the problem; this is the 3rd level of support. The following diagram illustrates the flow of problem reporting, tracking and resolution.



Coordination of Problem Reporting, Tracking and Resolution:

- All tracking is done through the Problem Reporting & Tracking Database
- Help Desk, Level 1 and Level 2 support will inform problem requester with status information and probable time of fix
- Problem Reporting & Tracking Database is a source of new requirements and system enhancements

2.20.1 Support and Help Desk

The policy of the Technology Sector is to provide responsive and efficient support for all hardware, networks, and software, and to resolve 98% of all problems within 24 hours.

Centralization of support is the stated goal of the Sector. Planning, recording and tracking of problems, and interfaces with vendors should all be performed with or through centralized resources. There will be one centralized Help Desk that will be contacted for all problems. The Help Desk will then attempt to help solve the problem, and if it cannot be resolved, it will dispatch the problem to the site Frontline.

Technology Sector will provide a 24 hour telephone Help Desk that will take calls for all system problems.

Technical support will be provided in the following areas, and technical support personnel will be trained to support one or more of the following:

- Hardware
- System software, database management system, operating system
- Application software, both Customs and non-Customs core applications
- Networks

The Technology Sector will provide Frontline (1st level) support for software, hardware, and network problems, at all ECA locations where systems are installed. In smaller sites one or two personnel may have to be trained to provide Frontline support in all of these areas.

As applications systems, databases, and the use of Web-based systems increases, and as systems become more technologically complex, some of the technical support provided at the Help Desk and level 1 will migrate toward the main processing center.

2.20.1.1 Levels 1, 2 and 3 Support

All problems are to be reported to the centralized Help Desk. The Help Desk will record, perform initial problem analysis, determine whether it is a hardware, software, operations, or network problem, attempt to fix, and dispatch the problem to a higher level if it cannot be fixed. The Help Desk will update the Problem Reporting and Tracking database, and inform the person reporting the problem of status and expected time to repair.

Level 1 is the Frontline, which is contacted by the Help Desk when the Help Desk cannot fix the problem. The Frontline support needed at the remote, satellite, or lowest levels in the network/node hierarchy will be primarily for PC and printer support, since the applications and the data will reside at the main center (s). The analysis done by the Help Desk will be used by the Frontline personnel to further analyze and fix the problem. Level 1 may contact the problem reporter and the Help Desk to further analyze the problem. Level 1 may contact the central support organization for assistance, without formally turning the problem over to Level 2; this turnover occurs when Level 1 cannot fix the problem. Level 1 will update the Problem Reporting and Tracking database with status, fix, and disposition information, and provide the problem reporter with an estimate of when the problem is likely to be resolved.

Level 2 is the technical support at the main data centers. Level 2 will perform additional analysis, further isolate the failing component, document the problem in detail, perform tests if required, and fix the problem. If it cannot be fixed at level 2 it is escalated to level 3. Level 2 is responsible for keeping the level 1 technician informed of problem status and in coordinating level 1 onsite problem resolution with level 3. Level 2 will update the Problem Reporting and Tracking database with status, fix, and disposition information, and provide the person reporting the problem with an estimate of when the problem is likely to be resolved.

Level 3 is the maintenance vendor for hardware, software, and networks. Level 3 and all of its extended resources will be called upon when the problem cannot be resolved by the Technology

Sector's technical support. Level 3 may require onsite problem resolution, which is coordinated through level 2.

2.20.1.2 Problem Reporting, Tracking, and Disposition

All problems should be telephoned to the central Help Desk, and are to be recorded electronically into a centralized Problem Reporting and Tracking System with name, date, time, description of the problem, and to who was assigned for initial analysis. Initial analysis will determine whether the problem is hardware or software and to whom it should be sent for further diagnostics. Additional information will be entered into the electronic system showing how the problem was resolved, when it was resolved, and who provided the repair.

As the problem is escalated to higher levels, it is electronically sent to the next level and additional information is entered into the Problem Reporting and Tracking System with the action and when it took place. In all instances the person originating the problem request should be notified of estimated time to repair the problem.

Tracking of problems and follow up with vendors is the responsibility of the technicians at the main center. The local site that initiated the problem call can provide additional details, but the coordination and communications should be done through the main center.

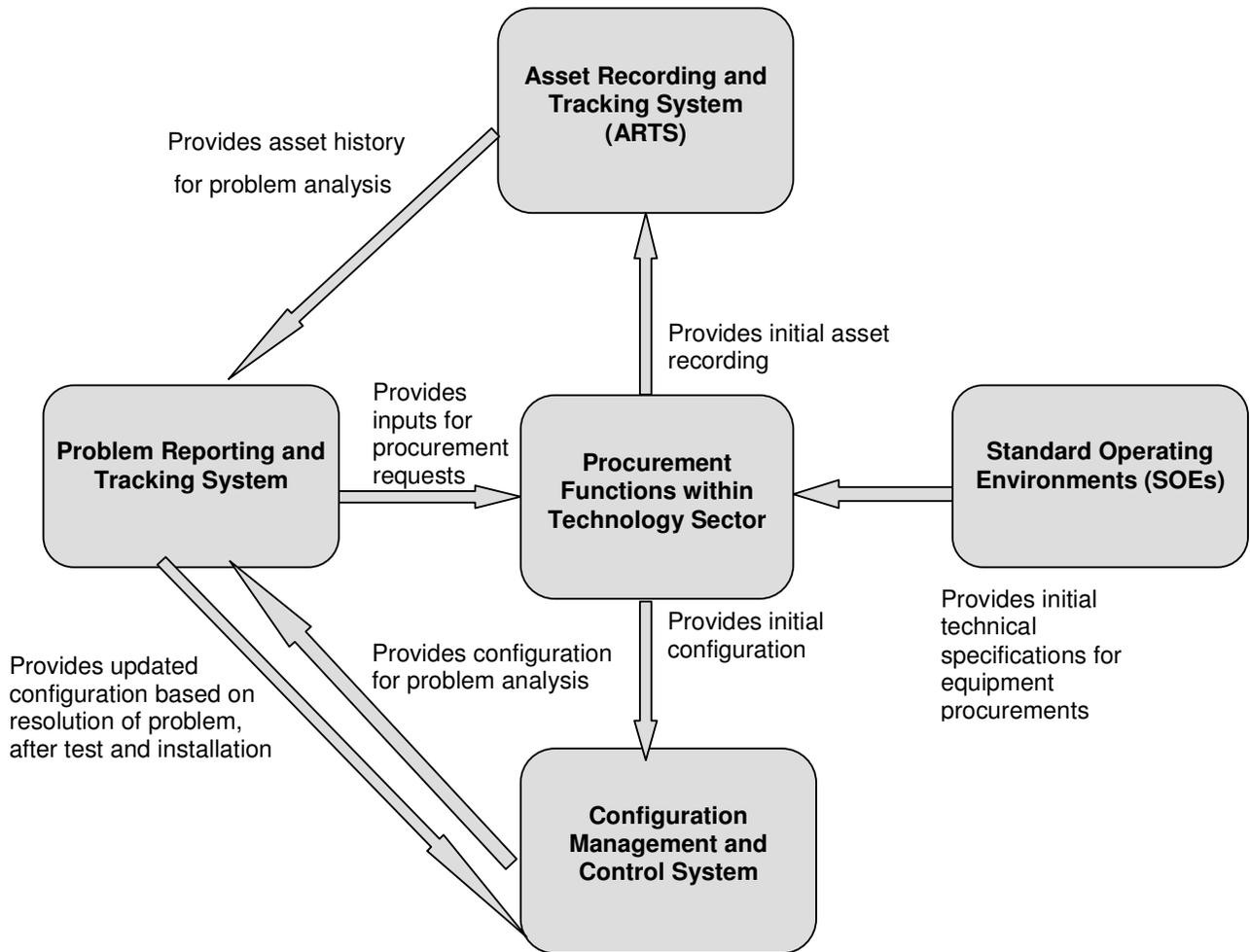
If a problem cannot be resolved within 3 business days by the vendor, then contracts personnel should be notified to review the Service Level Agreement terms with that vendor and determine if enforcement and potential penalties actions should be initiated.

By recording all problems in the Problem Reporting and Tracking System the main center has the complete historical database of all reported problems. This information should be analyzed every 3 months to detect specific recurring hardware or software problems, and also to identify specific hardware that may be experiencing a large number of problems and should be replaced because of this problem history.

Non-ECA users such as other governmental units, brokers, banks, and traders, experiencing system problems should contact the Help Desk at the Main Customs Site. The contact can be made by telephone or email. Onsite support may be provided if the reporting site is within easy driving distance of one of the IT locations. Every attempt will be made to resolve the problem without going onsite. If the hardware is owned not owned by the ECA, support will be limited to application software and the network.

The following figure shows how the various functions and databases work together in providing the Sector the information it needs for problem reporting, managing assets configurations, and procuring equipment.

Problem Reporting, Asset Management, Procurement, and Configuration Control



- **Problem Reporting system utilizes both Configuration Management and Asset Recording systems.**
- **Configuration Management and Asset Recording systems could be the same system, or different systems in which case their data must integrate.**
- **Procurement utilize SOEs, and the results of analyzing the Problem Reporting System for persistent problems that require replacement of equipment**

2.21 CONFIGURATION MANAGEMENT AND CHANGE CONTROL

It is Sector policy to maintain configuration controls over all IT assets. Hardware, software, and network components will have their configurations reported and controlled through the use of online software utilizing a configuration database. This software system may be the same as is used for Asset Tracking and Recording System (ARTS) or it may be separate, but it must be integrated with the ARTS system.

The purpose of configuration and change controls is to ensure the accuracy, integrity, authorization, and documentation of all changes. Configuration and change control procedures are to be used for all hardware, software, networks, and documentation.

Configuration and version levels are to be maintained for all assets, in all environments (e.g., production, development, test). The distribution of all hardware, software, and documentation updates should utilize configuration and versions controls, and are to be performed through a set of defined procedures.

All servers, PC's, routers, switches, firewalls, intrusion prevention or detection, authorization/authentication appliances, hubs, and other devices in the production environment are to be configured exactly or nearly the same. This applies to both hardware and software. The Asset Recording and Tracking System (ARTS) will provide the current configuration for any device. The Head of IT in each site is responsible for configurations, to ensure that the ARTS is properly updated, and to prevent non-standard configurations from being deployed. The standard configurations are defined by the Standard Operating Environments.

Only officially licensed software can be used on any ECA computer. The software and its configuration should be recorded in the Asset Recording and Tracking System (ARTS).

The Sector will define the detailed procedures for implementing version controls. The procedures must be documented, be repeatable, have been tested and approved by Quality Assurance, use automated tools, and properly record the history of the changes. A formal change request must be submitted to either Business Applications or IT Infrastructure who will evaluate the costs/benefits, risks, training and documentation requirements, and prioritize the change request. If the change is approved the solution including training and documentation will be planned; it will be tested and approved by Quality Assurance, and then combined with other requests into a version change package.

Changes can only be moved into the production environment after Quality Assurance has formally approved that the following Sector policies and procedures have been followed:

- The change has been approved by the PMO, the IT Governance Board, or the Sector Director
- A Change Request has been formally submitted
- Security safeguards and protection of data are satisfied
- Design reviews have been successfully conducted
- Testing at all stages and levels has been successfully completed and approved
- Documentation for systems, databases, and operations has been updated
- The change itself has been identified in the configuration management and control system, version and change numbers have been assigned, and the change has been incorporated in a larger change package (e.g., a version) if required.

2.22 QUALITY ASSURANCE

The role of quality assurance in the Technology Sector is to ensure that the formal policies, procedures, and standards are being followed. Q/A does not establish these, but it is empowered to

conduct activities to ensure that policies, procedures, and standards are being followed, and that informal ones are not being substituted for the formal ones.

Quality Assurance currently lies in the Business Applications Department. Consideration should be given to moving this function to report directly to the Central Directorate for TI & Communications because its role spans this entire Directorate.

Quality Assurance also must work very closely with the Sector's Operations Technology Initiatives department that coordinates and publishes standards.

Quality Assurance performs the following functions:

- Ensures that the procedures and policies of Technology Sector are being followed by conducting formal reviews as a part of every project.
- Ensures that there are naming standards for directories, entities, and data elements and that they are being followed.
- Performs audit functions to ensure that system development lifecycle, coding standards, documentation standards, and SOEs are being followed.
- Ensures that design reviews have been conducted successfully.
- Ensures that integration and system tests have been conducted successfully.
- Recommends and assists in writing new procedures and policies (the formal maintenance of procedures and policies is in the Financial and Administrative Affairs Directorate in the Technology Sector).
- Recommends changes and improvements to procedures and policies based on experience in applying the ones currently used.
- Trains personnel on the procedures and policies.
- Provides inputs to the Sector Annual Plan specifically for Quality Management.
- Is responsible for the movement of program modules or systems from Acceptance Test into the production environment, and ensures that code modules do not migrate from one environment until Q/A has reviewed the request and authorized the movement.
- Monitors production quality and problem reporting.

2.23 CAREER PLANNING AND ADMINISTRATION

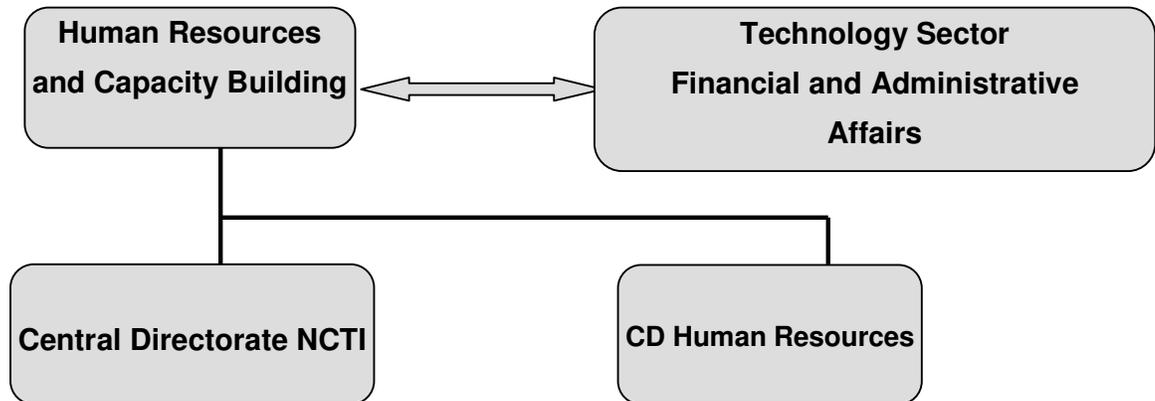
It is the policy of the Technology Sector to provide career movement, advancement, job enrichment, training, and objective performance evaluations for its employees.

The Technology Sector will promote an inclusive, supportive and innovative work environment that enhances business expertise, productivity, morale and professional development.

The Sector will produce an annual Personnel Plan consisting of positions and numbers of people in each position, skills requirements, training plans, and plan for recruitment and hiring. This plan will include a gap analysis comparing current numbers of positions and skills with what is required, and how the gap will be filled through promotions, training, hiring and other means. The Personnel Plan will contain tasks, dates, and responsibilities for executing and delivering the results.

Technology Sector will closely coordinate its efforts with and seek advice and direction from the Human Resources and Capacity Building Sector as show in the following chart.

Coordination of Technology Sector and Human Resources and Capacity Building Sector



Coordination of Technology Sector and Human Resources and Capacity Building Sector

- Career Planning and Development
- Staffing and Recruitment
- Annual Personnel Plan
- Training Plan, Needs, and Requirements
- Training Course Development and Delivery

2.23.1 Careers

The Technology Sector will require trained technicians in the following key positions. This is an initial list of positions that may change over time:

1. Project Manager
2. System Architect
3. Programmer/Analyst
4. IT Infrastructure Engineer
5. System Security Specialist
6. Database Administrator
7. System Administrator
8. System Integration Specialist
9. Senior Technical Support Specialist
10. Help Desk Specialist
11. Frontline Technical Support Specialist
12. Web Developer/Administrator

Position descriptions have been drafted for these positions. Logical career paths will be defined to illustrate potential career movement between these positions, including required competencies, skill levels, and professional levels to enter a position. Training required to move to the next level or to another position will be defined.

Examples of movement upward into higher skilled and higher paying positions are:

- Frontline Technical Support Specialist to Help Desk Specialist
- Help Desk Specialist to Senior Technical Support Specialist
- System Administrator to Database Administrator or to System Security Specialist
- Database Administrator to System Architect
- Programmer/Analyst to Project Manager
- Senior Technical Support Specialist to System Integration Specialist

Technology Sector's annual Personnel Plan should use these positions as a guideline, specifying the number of personnel needed for each position, where and when they will be needed.

There should be at least 2 grades within some of the positions. These will be used to create upward movement for Sector employees by providing for promotions, increases in salary, job enrichment, and the potential to acquire new skills. Those positions that require at least 2 levels are:

System Administrators

Frontline Technical Support Specialist

Programmer/Analyst

The different grades within a position are differentiated by years of experience in that grade, the attainment of key skill proficiencies, and the performance achieved as evidenced by the yearly appraisals.

2.23.2 Recruitment

Recruitment needs are to be identified by the Head of each department and provided to the Sector's Financial and Administrative Affairs Directorate. The annual Personnel Plan These needs will be incorporated into the annual Personnel Plan. During the year this plan will be updated on a quarterly basis. These needs and requests will be analyzed by the ECA CD Human Relations and the requesting department within the Technology Sector to determine a strategy for filling them. Every attempt will be made to fill positions from within the Sector. For those positions where the strategy requires external recruiting, the positions will be published on the GoE employment website, the ECA's website, and where funding has been approved professional organizations that can assist with searching an identifying potential recruits.

Interviewing recruits should be conducted jointly by CD Human Relations and the Head of the department originating the request. Criteria for evaluating candidates need to be developed.

2.23.3 Career Planning and Development (Workforce Planning)

It is the policy of the Technology Sector to promote from within, as long as the candidate meets all of the technical and professional requirements. It is recognized that bringing in new people is important in order to infuse new ideas into the organization. This has to be considered when an existing position becomes vacant or a new position is defined.

The Sector will recognize both horizontal and vertical movements within the Sector. This means personnel can remain within the same position and advance within it. Or an employee may move laterally or be promoted into a different position and thus increase breadth of knowledge or pursue a change in the basic work he or she performs. Movement between positions is encouraged because it spreads knowledge among more of the Sector personnel.

Each employee's annual performance plan should include a section that describes the career objectives of that employee and some specific tasks that will allow the employee to realistically meet those objectives. These tasks may include formal or informal training, technical certifications, successfully completion and demonstration of increased skills, and professional society participation.

The Sector Director will conduct an annual planning meeting with his Directorate Heads to develop the Personnel Plan that will include career planning and development items for salary adjustments, promotions, and training for the next year. This should be part of the yearly budget preparation process so that salary expenses can be forecasted, and so that the Sector can provide for the correct numbers and skill levels for the next year. This planning mechanism should take into consideration the employees' career goals compared to the overall position requirements of the Sector.

Exit interviews will be conducted for all terminated employees, whether the termination is voluntary or initiated by the Sector. The purpose of exit interviews is to understand the reasons for the person leaving, and then to address these reasons if it is deemed that this will correct deficiencies in the Sector career planning and development plans.

2.23.4 Training

Certifications and qualifications to maintain position status, be promoted to the next grade, and to potentially move on to the next position in the career track will be defined.

Training will be provided through vendor certified standard courses such as Microsoft, Oracle, Cisco, and others, leading to technical certifications. These will offered by the Technology Sector for its employees.

Key senior technical personnel will be responsible for designing and implementing in-house courses for junior technicians in order to improve their skills and increase the general technical knowledge within the Technology Sector. These courses will supplement, but not replace the formal vendor standard courses.

The Sector encourages membership and participation in IT professional organizations. This is an excellent way to increase awareness of new technology and its applications.

All employees are expected to obtain at least 16 hours of formal classroom training each year in technical areas that add to or increase an existing skill.

All personnel training, certifications, and professional memberships should be recorded in the Human Resources database. This information is to be reviewed annually with the employee during the performance appraisal. The employee is responsible for ensuring that this information is both accurate and current.

2.23.5 Performance Appraisal and Counseling (Performance Management)

It is the policy of the Technology Sector to have a formal performance plan and performance reviews for each employee. It is also the policy of the Sector that the employee should be involved fully in this process and should take ownership of both the approved plan and the achieved results of his or her performance.

In the beginning of each year employees are to draft their yearly performance plan, review it with their direct manager and get approval. The next level of management's approval is also required for the employee yearly plan. The goals or objectives should be stated in terms of the specific categories. The goals should be realistic, attainable, and relevant to the tasks assigned to that position and grade.

Performance appraisals (reviews) are to be conducted every 6 months. The objective of the 6 month and 12 month reviews is to accurately document goals and performance based on observations and feedback. The employee is to first do a self-assessment, and provide this to his or her manager. The manager will then write his/her assessment and review the results with the employee. The manager will then obtain the next level of management approval of performance appraisal and any recommendations regarding rewards, promotions, or corrective actions. These mid-year and year-end performance appraisals use an agreed upon set of goals established in the performance plan at the beginning of the year. These goals may be quantifiable and measurable such as a certain amount of training, a certain number of problem calls resolved; the successful completion of a major activity or task; or they can be qualitative in nature. Promotions and salary increases will be based on the yearly appraisal. The appraisal criteria are:

- General goals that compliment the department and sector goals. Examples are the contribution of the employee to increasing the overall ECA client satisfaction of the sector. Another example is the successful installation or implementation of a major system of which this employee individually or as part of a team has a role.
- Specific goals. These should be relevant to the employee's position and grade. Examples are systems implemented or installed or supported, where the employee has a key role that is measurable such as project lead, lead developer, technical support, or in-sector training programs. Another example is providing an innovative and new solution to a problem.
- Technical competencies and career development. Examples are acquiring a new technical skill or competency during the year, or increasing the level of skills in an existing competency.

Competency can be measured by attainment of technical certifications, and/or by comparative evaluation of the beginning and end of year of a competency or particular skill.

- Career development for the current year. Examples of this are goals that the employee must attain in order to be considered for movement to a different position, promotion in the position, or promotion to a different position. Career development goals that go beyond one year can be specified if there are measurable interim goals at the end of the current year.
- Training goals. Each employee should attend at least 16 hours of formal technical training each year. This is an example of meeting the goal. Training acquired beyond 16 hours that contributes to increasing required skills of that employee may lead to a higher evaluation score.
- Client satisfaction. Client feedback for this employee in terms of how responsive, how well the employee has contributed to the client's success in using systems, how well the employee has communicated and kept clients informed of problems and solutions, are examples of goals in this area.
- Conformance to ECA and Sector policies and procedures, especially security. This is a very important objective, where not meeting all of the security objectives will result in a lower evaluation score, and may result in penalties and even termination of employment.

During the appraisal process managers are to assign a value of 1 (lowest) to 5 (highest) for each criteria area. In general the values in qualitative terms are:

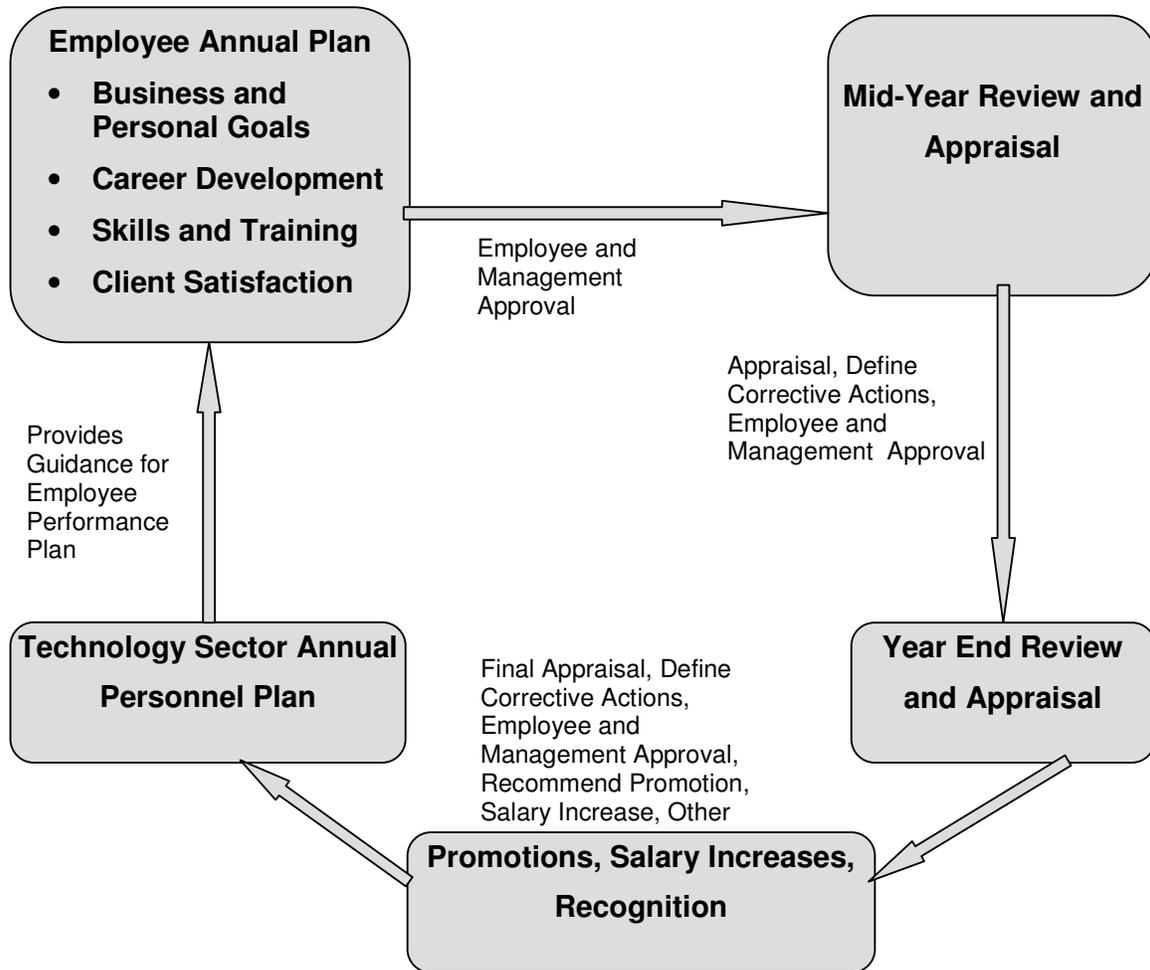
- 5 is a consistently exceeds the objective
- 4 is often exceeds the objective
- 3 is meets the objective
- 2 is meets the objective some of the time
- 1 is does not meet the objective

All managers should receive an annual briefing from ECA Human Relations on how to assist their employees in setting reasonable and achievable goals, how to conduct the evaluation, how to ensure fairness in evaluating employees in the same position and grade, and how to measure performance against goals in a consistent manner across their department and the Sector.

Throughout the year managers are to monitor employee performance and address any specific issues that are affecting their employee's performance. This may include changing goals where position changes, job assignments, and performance indicate that changes are required. Any interim changes to goals must be reviewed with the employee.

The following chart shows the general flow of the Performance Plan and Appraisal.

Employee Annual Performance Plan and Appraisal



- Employee Annual Performance and Appraisal Plan**

 - Sector Personnel Plan Provides Guidance on Goals for all Employees
 - Employee and Manager Agree on Yearly Performance Plan
 - Mid-Year Appraisal and Employee and Manager Agreement
 - Year-End Appraisal and Employee and Manager Agreement
 - Manager’s Recommendation for Promotion, Salary Adjustment, Other

2.23.6 Salary Administration and Promotions

The ECA Human Resources (HR) Sector will define and administer salaries and promotions. Technology Sector will recommend salary adjustments and promotions for personnel, within the guidelines and policies defined by HR.

Technology Sector will review sector salary and benefit structures annually, compare salaries and benefits with other government agencies, private and public companies, and make recommendations to Human Resources Sector on general salary level adjustments.

3.0 IMPLEMENTATION

3.1 HELP DESK IMPLEMENTATION PLAN

The Help Desk for the Technology Sector will be implemented over a period of time, to coincide with the installation of new IT infrastructure and the new centralized Customs Commission Automated System. The approximate time frame is expected to be 18 months.

The activities, milestones, and timeframes for implementing the Help Desk are described in the succeeding paragraphs.

3.1.1 Plan

- Determine the types and volumes of problems likely to be reported. Today these are primarily hardware and application software problems. As new infrastructure and centralized applications are implemented, the mix of problems is likely to change to more application software problems especially with the new Customs Commission Automated System, and to networking problems. Anticipating and/or determining the primary types of problems are essential in order to have the correct skills at the Help Desk. It is important to recognize that the types of problems will change over time, thus requiring new skills to be acquired for the Help Desk.
- Determine the hours the Help Desk will be in operation. The recommendation is to have it in operation for 2 shifts, 7 days a week. An emergency number must be provided for 3rd shift problem.
- Determine the skills and the number of personnel required for the Help Desk. The number of personnel is determined by:
 - Develop a problem call profile for each hour of the day, looking for the hours of peak problems, which typically is between the 1st and 3rd hours after the start of each shift. By assuming how much time it takes to record and start fixing a problem, an estimate can be made of the maximum number of Help Desk personnel needed at peak times, normal times, and periods of low activity.
 - Provide sufficient Help Desk personnel to record and attempt fixes for the peak hours. The initial estimate is 3 people for first shift and one person for 2nd shift.
 - Shift one and especially shift two should have planned contingencies for backup Help Desk personnel.
 - Determine the skills necessary to fix 70% of the problems reported to the Help Desk, based on estimates of the most likely problems.
- Determine the specific personnel who will be on the Help Desk. The skills required will provide the best initial guidance. If skills are not sufficient, a training program is required; or additional skilled staff may supplement the Help Desk until permanent personnel can be trained.
- Determine the requirements and the mechanism for problem management. This includes reporting, tracking, status, closing and maintaining history. It also includes defining categories or types of problems (hardware, networks, application software, user error, documentation, and data), severity, criticality, etc.
- Determine the infrastructure required to support an online Help Desk. This includes phone communication lines, data networks, backup networks and lines, Internet access, and an email system. Ideally VoIP should be used for the telephones since these can utilize the data network already or soon to be implemented over the Internet.

- Determine how the Help Desk and Level 2 support will interface with Level 3 vendor support. This may include online access to the vendor's problem reporting database, and/or online access from the vendor into the Technology Sector's Problem Reporting and Tracking database.
- Determine how problems will be reported. Initially it will be by phone, but that should change to using email as soon as the email system is available to clients. Phones should always be available as a backup mechanism.
- For any problem called in, determine what information is to be recorded, how it is to be recorded, and what procedures are used to update, track, and close the problem.
- Develop escalation procedures for the Help Desk for level 2 and 3 support, how to contact these higher levels, and under what circumstances. An emergency procedure is required for disasters or other highly damaging events.
- Develop procedures for keeping the client (person who reported the problem) informed of the status of the problem and the estimated time to resolve.

3.1.2 Develop or Procure

- Develop or procure software for problem management system. There are several in the market place that provide Help Desk and Call Center functions. Some of these include or have options for Asset Management and also Configuration Control. The software vendor selected for the new Customs Commission Automated System may offer software that the ECA can install; software that may tie directly into the vendors support structure.
- Develop or otherwise provide linkages and access to the Asset Recording and Tracking System, and the Configuration Control system.
- Procure the infrastructure required for the Help Desk. Most of the infrastructure will already have been planned or installed as prerequisites for CCAS. The primary infrastructure unique to the Help Desk will be VoIP phones and supporting call switching/management system, PCs with large displays to record problems, a server for the reporting system, and specialized audio equipment such as headphones.
- Develop a most Frequently Asked Questions (FAQ) list, with standard answers for the Help Desk personnel. This list should answer at least 50% of the reported problems.

3.1.3 Install Pilot

- Test and install infrastructure and Help Desk problem management software. Document operational procedures.
- Install and test Help Desk infrastructure.
- Test interfaces to the Asset Recording and Tracking System, and the Configuration Control System, and optionally to the vendors' problem reporting systems.
- Provide training for Help Desk personnel on how to operate the problem management system.
- Provide instructions and online help for pilot users.
- Install as a pilot program in Alexandria, a regional center and several of the satellites. Update procedures as a result of lessons learned during the pilot installation.

3.1.4 Deploy

- Complete the installation of Help Desk infrastructure at all sites.
- Provide instructions and online help for all clients.

- Go online with all sites.
- Provide problem history to the Business Applications and Infrastructure departments.
- Develop backup procedures so that the Help Desk can be moved quickly to the disaster recovery site.
- Improve the Help Desk function, system and procedures as a result of client feedback. Update the FAQ list.

3.1.5 Help Desk Implementation Time Line

The Help Desk can be implemented in phases. Ideally, the Help Desk should be fully operational in time to support the implementation of the new Customs Commission Automated System.

Although the Help Desk can be fully operational without the CCAS software, its full value will be realized only when this software system is fully installed. The Installation and Deploy phases are dependent on ETA's providing the infrastructure and the CCAS's software vendor delivering and installation the system within the 18 month timeframe.

The following chart is illustrative of how the Help Desk may be implemented.

Help Desk Implementation

Phase	Relative Month																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Plan	x	x																
Develop or Procure – Full function is dependent on CCAS vendor and installation			x	x	x													
Install Pilot						x	x											
Deploy							x	x	x									

3.2 IMPLEMENTATION PRIORITIES

The following chart lists the areas of policy and procedures discussed in this document; lists the relative priority; and provides descriptions and comments on the priority, its rationale, and dependencies.

The priorities are:

- 1 – meaning that the priority is very important and the implementation is immediate
- 2 – meaning that the priority is important and the implementation should be made within the next 6 months
- 3 – meaning that the priority is medium, and that the implementation can wait until months 6 to 12.
- 4 – meaning that the priority is not important at this time, and the implementation can wait until months 12 to 18.

Some of the priorities, although high, may have to be delayed because they are dependent on some other activity such as the implementation of infrastructure or vendor software. These conditions will be noted under Comments and Clarifications.

Recommended Priorities		
Area of Recommendation	Priority	Comments and Clarifications
Organization	1	This is required within now to provide guidance and direction for large infrastructure and CCAS procurements.
Relationships within ECA	1	Establishing these working relationships is important for planning the large infrastructure and CCAS procurements, as well planning for personnel and security.
Relationships to External Organizations	2	Establishing these working relationships is important for planning the large infrastructure and CCAS procurements, as well planning for personnel and security.
Management, Planning, and Controls	2	These are required to support the new organizational structure.
Sector Communications and Responsibilities	2	These are required to support the new organizational structure.
Key Performance Indicators and Measurements	4	Should be implemented so that Sector performance during the CCAS implementation can be measured.
Project Management	2	This is required to manage the CCAS vendor.
Technology Standards	2	This will be needed to manage the CCAS vendor.
Procurement	2	This will be needed to manage the CCAS vendor
Contracts and Vendor Management	2	This will be needed to manage the CCAS vendor.
Internal Audit	4	This is dependent on the new organization being in place and Internal Audit function being defined with resources in place
Client Satisfaction	3	This will be most important when Career Planning, and Key

		Performance Indicators are implemented
Security	1	This can be implemented immediately
Business Continuity	2	This is dependent on infrastructure installation
Email System	2	This will be required for full Help Desk support.
Asset Management	1	This can be partially implemented immediately
Development Standards	2	This is required by the time the CCAS vendor has started development, and may be stated or modified by the vendor.
Documentation Standards	2	This is required by the time the CCAS vendor has started development, and may be stated or modified by the vendor.
Testing and Procedures	3	This is required by the time the CCAS vendor has started development selected
Support and Help Desk	3	This is dependent on the new organizational structure being implemented. It may be delayed because of infrastructure (VoIP, email, hardware)
Configuration Management and Change Control	3	This may be dependent on CCAS vendor's configuration and control system and procedures.
Quality Assurance	3	This should be in place by the time the CCAS vendor starts development and implementation.
Career Planning and Administration	4	This is dependent on Client Satisfaction and Key Performance Indicators being implemented.

4.0 APPENDIX A

4.1 DATA CONFIDENTIALITY AGREEMENT

This data confidentiality agreement is to be given to each Technology Sector employee upon hiring, and then on an annual basis for their signature. Protecting the confidentiality of data within the Technology Sector is very important, and breaches of this policy will result in disciplinary action.

The Technology Sector may be allowed to provide ECA information only to an authorized individual and only to the extent allowed by the Government of Egypt and the ECA.

Section 1:

Customs information shall be confidential, and except as authorized by this agreement, no officer or employee of the Technology Sector of the ECA, nor any organization or person employed by the Technology Sector of the ECA who has or had access to the information, shall disclose any of the customs information obtained by him/her in any manner in connection with his service as an employee or other wise under the provisions of this agreement.

Technology Sector employees will exercise all due diligence in protecting Customs information. This includes: not removing any information from a Customs premise without written authorization from the Sector Director; not destroying any information without the written approval of the Sector Director; protecting documents, tapes, disks, diskettes, CD's and other media from any physical, electronic, or degaussing damage; securing and locking and keeping confidential Customs information when not being used.

Definitions: Customs information that must be kept confidential shall be that information submitted in support of a manifest, declaration, payment, audit, or investigation. This shall include an importer's or exporter's identity; the nature, source or amount of goods being declared, payments; receipts; credits; assets; liabilities; deficiencies; assessments; any information obtained in preparation for or during an audit or other investigation; or any other information received by the ECA with respect to a manifest, declaration or liability, penalty, interest, fine, seizure, or other imposition or offence. Customs identity means the name of the person or corporation, mailing address, and Customs identification number.

Section 2:

For all employees and other persons employed fulltime or as contractors, it shall be unlawful to willfully disclose to any person, except as authorized in this agreement, any ECA information as defined in Section 1. Any violation of this paragraph shall be a criminal offence, punishable upon conviction by a fine, or imprisonment, or both. If the offence is committed by an officer or employee of the ETA, he shall, in addition to any other

punishment, be dismissed from office or discharged from employment upon conviction of such offence.

Signed: by employee, contractor, vendor, or other 3rd party with authorized access to ECA information.

Date: _____

5.0 APPENDIX B

5.1 LIST OF REFERENCES

1. ITIL (the IT Infrastructure Library) for quality management, governance, project management, and standards
2. ISO9000 2000 series for quality management principles and quality assurance
3. BearingPoint ProvenCourseSM. The ProvenCourse methodology is a component of BearingPoint's ProvenCourse delivery framework and contains process, templates and techniques used to deliver BearingPoint services.
4. IRS Publication 1075, Tax Information Security Guidelines for Federal, State and local Agencies.
5. Network Working Group of the Internet Engineering Task Force.
6. United Kingdom, Office of Government Commerce, Governance, and Human Resources.
7. Egyptian Customs Strategic IT Security – Infrastructure Analysis and Recommendations. A report submitted to USAID by BearingPoint, Inc., June 22, 2006.
8. Egyptian Customs Interim Modernization Phase IT GAP Analysis. A report submitted to USAID by BearingPoint, Inc., February 5, 2006.
9. Egyptian Customs Authority Organizational Realignment. A working document of the ECA, approved December 6, 2005.

5.2 CRA VISITS AND MEETINGS

The following CRA and MoF consultants were contacted at various times during the writing of this document:

- Mrs. Iman El Kouny, Executive Consultant Customs Reform, at various times from June 12 through August 10, 2006.
- Mr. Alla, CRU in Alexandria, June 19.
- Mr. Shashika, IT Manager, Alexandria IT Processing Center, June 19, 2006.
- Mrs. Najury, Head of IT Reform for IT, Alexandria, June 19, 2006.
- Mr. Abdul Salam M. Al-Husseiny, Chief of Customs, Eastern Region (Port Said), June 21, 2006.
- Mr. Mustafa, General Manager IT Department, Port Said, June 21, 2006.
- Mr. Quenawy Abu Zaid, Head of Central Directorate, Suez, June 22, 2006.
- Mr. Nabil El Hofiy, General Manager of IT Department, Suez, June 22, 2006.
- Mr. Abel Hady, Head of IT Maintenance and Operations, Suez, June 22, 2006.
- Mr. Mohamed Mohamed Said Ahmed Mohamed, General Manager, Ain El Sokhna Customs, June 22, 2006.
- Mr. Amr Mohamed Gamal, Application Lead IT Department, El Sokhna Port, June 22, 2006.
- Mr. Reda Khaled, IT Manager, El Shokhna Customs, June 22, 2006.

Technical Assistance for Policy Reform II
BearingPoint, Inc.,
8 El Sad El Aali Street, 18th Floor,
Dokki, Giza
Egypt
Country Code: 12311
Phone: +2 02 335 5507
Fax: +2 02 337 7684
Web address: www.usaideconomic.org.eg

Technical Assistance for Policy Reform II
BearingPoint, Inc,
18 El Sad El Aali Street, 18th Floor,
Dokki, Giza
Egypt
Country Code: 12311
Phone: +2 02 335 5507
Fax: +2 02 337 7684
Web address: www.usaideconomic.org.eg