

GLOBAL MANAGEMENT SYSTEM

79. The legacy computerized applications being used by WHO were increasingly being found to be unable to deliver in a timely manner the information needed for effective and efficient management and administration of the Organization's programmes. In order to improve operational efficiency, streamline processes and effectively decentralize authority and responsibility, it was decided to replace the fragmented computerized information systems with the Global Management System (GSM), an integrated system for global management and administration, based on Oracle E-Business Suite. GSM was authorized by the Fifty-sixth World Health Assembly in May 2003 with a budget of US\$ 55.5 million. Later, in March 2007, it was decided to adopt a global service delivery model through a global service centre, to be implemented concurrently with GSM. A global service desk is to provide functional and technical support to the GSM users. M/s Satyam was selected as the System Integrator (SI) for the project, which is scheduled to go live on 3 June, 2008.

80. A detailed study of the project processes and preparedness for implementation of GSM was conducted at WHO headquarters in January–February 2008 to examine whether the GSM application development and implementation processes have adhered to the best practices and procedures including risk management and controls, and to review preparedness for the implementation of the GSM application. The audit was based on a detailed risk analysis and was conducted in accordance with the CoBIT¹ framework. On conclusion of the audit a Management Letter containing the audit findings and recommendations was issued to the Secretariat and the response of the Secretariat obtained. These findings, recommendations and the Secretariat's responses are discussed in the subsequent paragraphs.

Project management

81. For a major business project like GSM, which seeks to replace the existing work process of WHO by harnessing technology and doing substantial business process reengineering, it is important to ensure that the project achieves its deliverables with the given functionality within the estimated cost and the time frames envisaged. The time schedule needs to be worked out taking into account critical path processes. It was seen that the project, which was initially to go live in September 2007, was given the first extension until December 2007, then a second until March 2008 and a third until June 2008. The project management stated that a delay of nine months in a project of this magnitude was not viewed as a failure. However, three revisions of deadlines within a year put enormous pressure on the supporting personnel and structures for the project as they have had to constantly keep revising their plans and allocation of resources.

82. The benchmark to be used for project management was PRINCE2² methodology as per the Project Initiation document and the implementation of the phases of the project was required to be guided by Oracle's Application Implementation Method (AIM) and Project Management Method (PJM). It was seen in audit that the PRINCE2 methodology was not followed in toto and only a few forms and registers were maintained; AIM for oracle implementation was also not followed in its entirety and the key delivery phases recommended by the System Integrator (SI) were not perfectly

¹ CoBIT is an internationally accepted IT governance framework that allows managers to bridge the gap between control requirements, technical issues and business risks.

² Projects in Controlled Environments (PRINCE) is a project management methodology. It covers the management, control and organization of a project.

aligned with the AIM phases. Consequently, the project has been moved into the testing stage without satisfactorily completing the preceding stages. Management stated that the GSM project was using the best parts of the PRINCE2, AIM and Satyam's methodologies. It accepted that the key delivery phases recommended by the SI were not perfectly aligned with the AIM phases.

83. I recommend that an independent third-party technical acceptance of the solution before go-live may be considered, in the light of the project going into the testing stage without satisfactory completion of previous stages. Management has accepted the recommendation.

84. The project was being managed within a budget of US\$ 55.49 million. However, the costs of many activities directly attributable to GSM implementation including, inter alia, organizational change, global service desk etc., totalling US\$ 28.4 million, were not reflected in the project costs of GSM but have been provided in the regular budget of the Organization. The project management accepted that the costs mentioned by audit were not budgeted within the GSM budget of US\$ 55 million. It further stated that the global service desk and global service centre were in fact separate projects and other costs were considered as part of the normal operating budgets. However, these costs have been incurred for GSM and hence are directly attributable to the project cost and should be shown as such. The running cost for GSM and its support services for the next two bienniums is estimated at US\$ 48.8 million, and for the service centre operations at US\$ 3.5 million per biennium.

85. As per the Project Initiation Document, tolerance is defined as deviation from the required timeline or quality (for example - permissible delays/quality of software) by the GSM project team, and associated vendors. The level of tolerance was to be defined at each phase of the project, and the results monitored regularly. It was seen in audit that tolerance has not been defined in the form of permissible delays or the quality of software in each phase of the project and neither were these reflected in the Project Board minutes. This carries a risk of failing to obtain the desired quality of software within the envisaged timeframe.

86. Audit was informed that the programme management team was involved directly with Health Action in Crises (HAC), the technical unit most responsible for emergencies (HAC) during the development of their Standard Operating Procedures, and in 2007 a series of workshops with health technical units (HTUs) had demonstrated the system and communicated changes. However, audit found in interactions with HTUs that Management's perception that HTUs were heavily involved was not shared by the units themselves. They felt that their level of preparedness was not satisfactory; their involvement in the pilot projects and the user acceptance test was minimal and the outcome of their concerns about the desired flexibility and prioritization of their transactions for emergency responses has not been communicated to them.

87. The objective of regression testing is to thoroughly test the GSM solution with all the fixed codes, configurations, security profiles and responsibilities. This provides an opportunity to perform End to End¹ business integration testing (within E-Business Suite) to stabilize the solution before entering into further phases including the user acceptance test. It was seen in audit that the outcome of regression testing from the perspective of end-to-end business integration, based on the scenario identified and mutually agreed upon with the System Integrators, would not be benchmarked in the absence of detailed expected results before go-live. This is a risk factor against the stability of the solution. Management stated that the detailed test results for the regression test were the same as the

¹ End to End refers to initiating a process and completing it, such as a travel request or procurement request.

Pilot¹ project and confirmed that some scenarios had not been tested from an end-to-end perspective. However, it may be noted here that detailed expected results for functionalities which were not even envisaged in the Pilot cannot be extrapolated to the regression test.

88. I recommend that the GSM solution may be fully tested with all fixed codes, configurations, security profiles and responsibilities to confirm the stability of the solution before go-live. Management has accepted the recommendation.

89. It was seen in audit that no parallel runs were planned to be conducted for any module except Payroll at the time of GSM implementation. Even the Payroll parallel is being conducted using earlier months' data and using an instance² altogether different from that which will be used in User Acceptance Test or that will prevail in a live situation. The legacy data are being used to test the calculation accuracy of the GSM system and are not a full time logistics run for time and volume. This carries a risk of the outputs of the GSM solution not being validated against real-life scenarios.

90. I recommend that validating other modules in addition to Payroll may be considered against the legacy outputs before go-live to ensure the accuracy of outputs of GSM application modules. Management has accepted the recommendation.

Contract management

91. At the time of entering into the Oracle agreement it was recognized that "hosting services" would be required in order to cover the period prior to engaging a System Integrator to cover the "vendor fit-gap" exercise, and might continue to be required. This was sought to be achieved through Oracle On Demand. It was subsequently recognized that cost savings could be achieved and operational control and responsibility improved through separating the hosting of the development from the application support and extending Satyam's responsibility to include support of the development. In the event, the Organization opted to have the application hosted with International Computing Center and responsibility for the development of the application was given to Satyam. These were achieved through a "Change Request" under the contract. Management pointed out that as a result monthly cost has been significantly reduced and a competitive bidding exercise would not have made sense.

92. In this context it may be borne in mind that as per the contract a "Change Request" is a request to change or add to the services or performance standards. Hosting is completely different from making any change or addition to services. Further, the WHO Manual stipulates that only the Contract Review Committee has the authority to waive any of the procurement rules. While audit appreciates that the award of the work has saved money, awarding a major contract like the hosting contract as a change request technically contravenes WHO regulations and is also not in accordance with the contract with the System Integrator.

93. The contract of USS 27 195 000 with Satyam included performance of services i.e. technical activity for 15 000 person days. According to the original plan of work, the programme initiation, completion and end of warranty period were scheduled for October 2005, July 2008 and October 2008 (indicative) respectively. The go-live for headquarters has since been revised to 1 June 2008.

¹ Pilot refers to the Conference Room Pilot, a pilot project carried out at an early stage of the GSM project.

² An instance is the software (and memory) that Oracle uses to manipulate the data in the database.

Until now, Satyam has carried out technical activities for 21,131 days and thereby may claim a total of US\$ 28.6 million, exceeding the contracted amount by US\$ 1.4 million. There is a possibility of this amount rising further with more delays. Management, while recognizing the risks of further costs resulting from potential claims associated with delays, asserted that the contract with Satyam was a fixed-price contract and claims for delays were not automatically acceptable. However, the fact remains that there is a risk of cost escalation resulting from delay claims in respect of the System Integrator contract.

94. The authorized budget of US\$ 55.49 million for the GSM project includes US\$17.6 million for staff. There is a risk of incurring further costs associated with further delays. Any delay in the initial go-live will require the continuation of the full team (at an approximate cost of US\$ 340 000 per month). Any delay after the initial go-live will require the extension of a smaller team (at an approximate cost of US\$ 250 000 per month). Additionally, there are ongoing costs of hosting, third party software support costs and general costs estimated at US\$ 60 000 per month. The project management's efforts to manage such risks through staff planning with suitably timed roll-offs of concerned personnel are encouraged.

Solution readiness and User Acceptance Test

95. User Acceptance Test (UAT) is a very crucial phase in the project life cycle of major IT projects and should be initiated after the solution is completely and fully ready, to test all interlinkages and reports, as it is on the basis of this testing that the users give acceptance to the solution. It was seen in audit that the UAT has been initiated without the solution being 100% ready. Solutions related to workflow monitoring, project security setup, SSA-related customizations¹ as well as eight important reports that were not made available for UAT. Thirteen more reports were to be made available to UAT three weeks after the start of UAT. Acceptance by the business owners of these functionalities not being available for the UAT gives rise to a risk of having a solution that has not been tested fully in all dimensions by the users. Management stated that these components would have minimal impact on the overall solution and over time additional components and fixes would continue to be added to the GSM even after the system has been commissioned.

96. The reply needs to be viewed in the light of the fact that changes before production and changes that are made in an IT system after production are completely different in nature, one being a part of the overall system design and the associated interdependencies between various components, the other being generally incremental and limited in nature on an already established and working solution. The go-live deadline needs to take into account the lead times for various phases and the prerequisites for moving from phase to phase.

97. In the UAT, only partially converted and largely constructed data are being used and the business owners have agreed to run UAT without fully converted data. This leads to the risk of testing the solution without real data and not being able to replicate a real-life situation. The Organization's own Information Technology and Telecommunications (ITT) wing had also raised concerns and pointed out risks of not using fully converted data for UAT as a rigorous UAT should be a mirror of production. Management in its reply stated that UAT was based on a statistically sufficient and representative set of data constructed from a combination of converted legacy data and constructed data. However, it was seen in audit that in the UAT even for a crucial module such as payroll for short-term staff, only 25–30 cases were being used per region. Thus the UAT, in which partially

¹ SSA: Special Service Agreements.

constructed data without extreme boundaries that may actually be encountered after go-live are being used, may not give full assurance about the complete functionality of the solution. This is important as the cutover¹ and other testing would not involve users and this is the last opportunity for the actual users to be involved in the testing.

98. As the UAT is being conducted with partially created and partly converted data I *recommend* that during cutover ensuring fully converted, reconciled and validated data may be considered before go live. Management has accepted the recommendation.

99. In the UAT some users have been given more than one role, as both the initiator of a transaction and the approver of the same. This does not test the segregation of duties principle, as objectivity in approving a transaction when not initiating it cannot be tested by using this methodology. This control is a vital element in the system of checks and balances in the post-go-live scenario and not testing it leads to risks. In reply, Management stated that during UAT the approval process was being tested, including the segregation of duties principle, but did not elaborate on how it was being done.

100. It was seen in audit that only normal GSM business processes were being represented by the End to End scenarios. UAT does not allow any new End to End scenarios to be introduced and the data are to be tested in the normal limits. This makes it a very limited UAT for normal circumstances with normal data, whereas in real-life scenarios, because of the nature of its activities, WHO may need to work in very extreme circumstances, for example, mobilizing large amounts of money in a very short time for emergencies.

Organizational readiness and training

101. The health technical units run a few of their own IT systems which have been developed and are being maintained by these Units. These IT systems need to be connected to the Global Data Hub for obtaining information from GSM to be able to function/generate reports. It was seen in audit that the status of the remediation of applications running in HTUs, which are to be read from the Global Data Hub, was not clear and they would not be tested during UAT using real data. Management stated that it sought to minimize the risks to the Organization by ensuring extensive and regular communication and support on this matter. However, the related critical issues and remedial actions for those were found, in audit, to be undefined. If these are not addressed in time then the risk of these systems, which generate reports for the HTUs, not being able to function in the post-go-live scenario remains unaddressed.

102. The responsibilities of the global service centre (GSC) include global administrative processing, i.e. global payments, global payroll, global human resources, global procurement, global application support (including GSM database administration and GSM application maintenance), global service desk support (including first- and second-level GSM functional and technical support and tracking), and GSM system administration. It was seen in audit that the capacity planning for the global service desk applications at GSC had not been done. The existing bandwidth is sufficient only for diagnostic information collection. If remote PC screen shots are required this will require more bandwidth allocation. Further, no bandwidth increase has been done either for the regional or the country offices and there was no documented plan for a network application profiling exercise for Global Data Hub

¹ Cutover: The process of transferring existing data, functions, or users of a computer system to new facilities or equipment in a synchronized manner.

applications, without which bandwidth requirements cannot be estimated for GSC and other remote offices.

103. Management's decision that a firm business continuity plan for the GSC will be in place before go-live in June 2008 is appreciated. However, an effective business continuity plan needs to be preceded by a risk assessment to define the mission-critical functions and data, the systems supporting them and the impact that their unavailability will have on WHO. It also requires coordination with external parties such as the suppliers of hardware, software and communications service and equipment. It was seen in audit that in the absence of a formal, documented and tested disaster recovery plan, business continuity of the automated processing in GSM, in the event of a major disaster, remains at a high level of risk with significant implications for the working of critical areas of the Organization.

104. I *recommend* that a firm, documented and tested disaster recovery and business continuity plan for the global service centre may be put in place before GSM and GSC go live. Management has accepted the recommendation.

105. The global service desk (GSD) has been established as a single point of contact for information relating to global administrative processing and problem resolution. Since GSD will provide service through remote access of both a business-related and a technical nature, the staff employed in GSD should have the technical capabilities for problem resolution and the centre should have enough bandwidth. It was seen in audit that the staff who would work for GSD were largely newly recruited staff having limited technical knowledge. Therefore their institutional knowledge about the legacy system would also be constrained. It is proposed that this be managed by training in GSM, Oracle systems and in the subjects by subject matter experts, but staff would largely be learning by handling problem resolution. However, it was seen in audit that there was no involvement of the GSD in the User Acceptance Test. Management stated that it was reviewing a proposal by Satyam for second-, third- and fourth-level GSM support during a transitional period after production cutover and GSD staff would be working closely with Satyam during this period; regional offices were also establishing transition service desks to support post-cutover. The reply underscores the risk of overdependence of the Organization on the System Integrator in a post-production scenario.

106. A lack of documented training need analysis (e.g. an analysis of skill requirements and skill gap analysis) and training need identification (e.g. number of staff to be trained for GSM, role-based training to be given to the staff etc.) for the officials of WHO to prepare them for the post-go-live scenario was noted by audit. It was further seen that the training for the staff of the global service centre (GSC) has begun adopting the approach of "Training for trainers", as trained staff members will train other staff at GSC. However, no Trainers' Manual, with structured modules for training delivery or Users' Productivity Kits (UPKs) for transition had been prepared at the time of audit. This indicates a lack of uniformity in approach towards training delivery methodology. Management stated *inter alia* that instructor manuals were an output of the UPK tool and GSM trainers would be provided with guidelines. However, audit would like to point out here that the UPK is a trainees' manual, not a trainers' manual and that guidelines cannot take the place of detailed manuals.

107. I *recommend* that documented training-need analysis, training-need identification, a Trainers' Manual and Users' Productivity Kits may be put in place before go live, with adequate training imparted to GSM users for the post-go-live scenario. Management has accepted the recommendation.

Knowledge management

108. Given the recurring high volume of work in maintaining the legacy systems, the ITT personnel of the Organization could not be fully associated with the GSM project. Thus there is a limited and insufficient transfer of knowledge of the GSM solutions from GSM and the System Integrator streams to ITT. There is limited organizational knowledge within WHO of GSM functionality, apart from the GSM Project Development Team and the System Integrator; there is no evidence of a formalized, detailed plan for knowledge transfer between the current systems integrator and the ITT, the post-go-live holders of GSM. Management noted the audit observation and stated that it was WHO long-term strategy to continue out-tasking to a third party vendor (offshore) the technical support of the solution and thereby minimize the need to transfer and sustain detailed technical knowledge of the solution in-house. It gave assurances that as it worked to negotiate the support contract, the risks of over-dependence on the System Integrator, observed by audit, would be given full consideration.

109. I *recommend* that a formalized detailed time-bound plan for detailed knowledge transfer between the System Integrator and ITT may be put in place. Accepting the recommendation, Management stated that the required knowledge transfer would be undertaken during the roll-out and stabilization period.

Data conversion, cutover and transition

110. It was seen in audit that the complexity and scale of work on data conversion have been underestimated or not appropriately prioritized by the GSM project management; the conversion strategy had not been followed consistently and the actual work did not follow the methods laid down in the conversion document. Management stated that the conversions required for GSM were indeed complex and resource constraints delayed the completion of some of the detailed conversion documents. It further stated that the conversion strategy as outlined in the conversion document had been followed with a few exceptions. However, it was seen in audit that a number of critically important documents have still not been designed.

111. It was seen in audit that data availability by businesses included new data which would have to be created and which did not exist in the legacy systems. This requires manipulation and creation/manufacturing/assembling of electronic data. Specifically, there are challenges in the programme and finance units' data conversions where workplans need to be finalized, approved, linked with HR costs and prepared for conversion testing. The slippage in these areas may have an adverse impact on the cutover and the schedule of go-live. Management stated that the above fact has been highlighted as a risk to all stakeholders.

112. It was seen in audit that no historical data would be converted/transferred from WebBuy, the existing procurement software in WHO; it will continue to be available in WebBuy and can be accessed only until WebBuy is shut down. It was considered by Management that a database would be built up in GSM in a few years. This carries a risk that trend analysis of past orders and vendor and supplier performance evaluation will not be possible. Management stated that in addition to the limited benefits, converting historical purchase orders into GSM was not a simple task, and as a result of this complexity, purchase order data in WebBuy would be made available as part of the legacy decommissioning and data archiving strategy. However, as no data warehousing functionality is proposed for the historical information contained in GSM and the legacy decommissioning and data archiving strategy are still to be finalized, the loss of institutional memory of the Organization is a real risk in the post-go-live scenario that needs to be taken note of.

113. I *recommend* that making historical information available to the businesses through a suitable interfacing mechanism between the legacy WebBuy and the GSM, in consultation with the business-owners, may be considered. Management has accepted the recommendation.

114. It was seen in audit that data validation was not explicitly embedded in the GSM project and there was no formal data integrity testing. Normally data should be reconciled and certified by business owners. It was observed that insufficient time was allocated for this activity in the project plan. From interaction with users it was understood in audit that some validation was expected but details of sample size and the period during which validation would be done was not clear. There was no evidence of estimation and planning that quality assurance of the converted data (i.e. validity and integrity testing by business owners) would take place.

115. Though Management stated that the risk about quality of data was being mitigated in the cutover processes, a study of the official cutover document revealed that in many cases, for objects which determine important transactions (duty stations, locations, travel events, suppliers, items, purchase orders, allotments, programme budget etc.) the acceptability criteria were described in generic terms and most depended on count tally and random sampling. Business plans on how to do the detailed reconciliation and sign off were unclear. As this would be the last opportunity before data is finally loaded into the GSM for actual running in the post-go-live scenario, such limited testing of quality of data is a risk which may later require remediation when the system is operational.

116. I *recommend* that Management may consider defining in specific and detailed terms the reconciliation and validation methodology for converted data, with concrete statistical inputs, to be adopted by businesses, before uploading the converted data in the GSM for go live purposes. Management has accepted the recommendation.

117. The legacy system decommissioning is the practice of removing a system (application, database and/or platform) from service, while retaining access to the business-critical data housed within that system. There was no evidence of finalization of a strategy for legacy system decommissioning and a database archiving. If the legacy systems are not decommissioned effectively and efficiently, there could be significant future additional costs to WHO in terms of hardware, software, human resources and infrastructure. Moreover, considering the fact that for some functional streams only the balances are being taken into the system and not the full historical data (e.g. Procurement), the risk of loss of institutional memory and its impact on the decision-making processes remains high. Management gave assurances that as it worked to finalize the strategy the risks observed by audit would be considered and an interim strategy would be in place to facilitate the cutover to the GSM and to outline the mid-term archiving strategy.

System security

118. It was seen in audit that though there was a WHO Global Information Security Document which covered high-level overarching security policies, the related processes were not detailed and no formal Information Security Management System (ISMS) was in place for the GSM environment, including the global service centre. This is a major risk area, especially for GSC, where major transaction processing will take place which will have linkages with GSM servers and with regional and country offices. Management stated that WHO was developing an ISMS and gave assurances that it would soon draft, coordinate and obtain approval of several mainstream policies that would set the background for the day-to-day security decisions and processes.

119. An enterprise resource planning (ERP) system such as GSM has a large number of users accessing the system and large volume of transactions per employee. There are risks associated with the sharing of information with third parties such as suppliers by the linking of systems. As a result of the above, ERP systems, while bringing about increased efficiencies through the streamlining of business processes and significant reduction or elimination of manual processes, need to have appropriate security controls built into them.

120. Audit appreciates that security development and testing have always been considered by Management as integral to the different phases of the project in which security components were put in place and tested as part of both the Pilot project and the User Acceptance Test. Further, Management has stated that there was an in-built security mechanism in the Oracle application, database level security was in place, and operating system level access was controlled and limited. However, in the absence of a properly documented and tested plan, the evaluation of effectiveness of the system's security features and identification of any weaknesses, including penetration testing for network security, and their mitigation, remains to be addressed.

121. I recommend that the evaluation of system security including penetration testing may be carried out rigorously and documented. For this, engaging an independent third party may be considered. Management has accepted the recommendation.

Conclusion

122. The audit review flags a number of risks in areas of project management and the ongoing preparatory exercises and tests leading up to the commissioning of the GSM. Though it cannot be asserted with certainty at this stage that the risks will manifest themselves in breakdowns or stalling of the system on commissioning, if left uncovered they may render the system vulnerable, even necessitating costly rectifications at a later stage. Management has indicated its acceptance of the recommendations, which is a welcome step towards mitigating the risks.

123. The above recommendations relating to global service management are accorded high priority. Management has accepted the recommendations.

CASES OF FRAUD AND PRESUMPTIVE FRAUD

124. During the biennium there were seven cases of proven fraud involving US\$ 235 235. I am pleased to note that necessary administrative actions have been completed in these cases, with two cases remaining subjudice. Other cases of presumptive fraud have been reported and investigations have been launched by Management into these cases. Progress of investigations and actions taken will be monitored in External ~~Audit~~

