Auditing Systems Development

This paper is an exposure draft of a new major output of the INTOSAI Working Group on IT Audit, produced by a research team from the SAIs of China, Kuwait, Pakistan and Bhutan. Readers' comments would be very much welcomed by the team. They should be emailed to cnao@audit.gov.cn or amycnao@yahoo.com, marked for the attention of Ms Yang Li of the Chinese National Audit Office.

As Information Technology has advanced, Government organisations have become increasingly dependent on the use of IT to carry out their business operations and service delivery and to process, maintain and report essential information. Organisations often spend significant resources in developing, acquiring and maintaining application systems that are important to their effective functioning. These systems in turn manage critical information and should be considered an asset that needs to be effectively managed and controlled.

But heavy reliance on IT can also result in unacceptable levels of disruption if the systems development is delayed or does not work as intended. Many risks can, to some extent, affect the successful development or acquisition of a new information system. These include the risk that the system will:

- never be delivered;
- be delivered late (time overrun);
- exceed budget (cost overrun);
- divert user resources to an unacceptable degree;
- not deliver the required functionality;
- contain errors;
- be unfriendly;
- fail frequently during operation;
- not perform to the required standard;
- be difficult and costly to operate, maintain and expand;
- not interconnect with other systems.

The investigation of these IT project failures revealed a number of common problems, which can be summarised as follows:

- Failure to assess (and manage) project risks, in particular stemming from:
  - an unrealistic business case;
  - technology problems;
  - lack of senior management involvement;
  - lack of user commitment to the project.
- Ineffective project management:
  - inexperienced IT project managers;
  - failure to apply, or an inadequate, IT project management methodology;
  - lack of quality standards;
  - vague or incomplete specification of requirements;
  - failure to streamline the requirement specification, resulting in slipping deadlines and rising costs.
- Mismanaging consultants and suppliers:
  - failure to seek competitive tenders;
  - high staff turnover – no continuity;
  - vague terms of reference for consultants and open-ended contracts;
  - failure to monitor and control consultancy costs;
  - lack of independent quality assurance on consultants' work.

- System implementation failures:
  - unrealistic delivery deadline;
  - inadequate acceptance testing;
  - taking shortcuts due to lack of time (particularly cutting back on training, testing and quality reviews);
  - unworkable or non-existent contingency plans.

The risk of project failure can be dramatically reduced by breaking down the project into a number of manageable stages, and where the aim of each stage is to produce one or more pre-defined products. The method typically used is the System Development Life Cycle (SDLC), which is a process involving multiple stages (from establishing the feasibility to carrying out post implementation reviews), used to convert a management need into an application system. It is custom-developed, purchased or a combination of both. The advantage of a structured approach is that it helps to reduce the complexity of planning, monitoring and control. It also offers a number of points during the project where progress against pre-defined deliverables can be reviewed and corrective action taken as necessary (including abandoning the project!).

To ensure a structured, cost-effective and efficient audit of a systems development project, a new approach should be undertaken. This new approach involves the auditing of each completed phase of a system development and giving input that allows corrections to be made before next phase of the development. This approach differs from the traditional audit approach of auditing systems development projects only after the project has been completed, the focus of traditional audit is on auditing the completed systems development process to assess if the development took place on a structured basis.

The IT auditors' overall objective, like everyone else involved, is to contribute to the success of the system project. IT auditors are best qualified to do this by helping control the 'exposures' resulting from the project, and giving management reasonable assurance that this has been done.

1. Audit plan

When auditors begin auditing the work of SDLC, they should first prepare an audit plan. A good plan will be a good beginning. In the audit plan, the auditor should identify the audit scope, determine audit objectives, gather basic information about the organisation, determine materiality, assess risk, and evaluate internal controls.

During the planning, auditors should communicate with the organisation for audit objectives, and to get relevant information about its information system, technology infrastructure, structured approach used for developing application system, organisational structure, IT strategic plan etc.

Auditors should also have an understanding of the above information, establish levels of materiality, make assessment of risk, and take into consideration of internal controls of SDLC.

While planning the review of the SDLC of an application system, auditors should consider:

- The acquisition/development mode, technology, size, objectives and intended usage of the application system;
- Project structure for acquisition and implementation;
- Skill and experience of the project team;
- The SDLC model chosen;
- The formal SDLC methodology and customised process design adopted, if any;
- Risks that are likely to effect the SDLC;
- Any concerns or issues perceived by appropriate management;
- The current SDLC stage;
- Any prior review of the earlier SDLC stages of the application system;
- Any prior SDLC reviews of similar application systems;
- Any other risk assessments/reviews by the IT auditors or others (such as IT staff) that have a bearing on the proposed review;
- The skill and experience level of the IT auditors available and the possibility of getting competent external assistance where necessary.

Identify audit objectives

An SAI gets its authority from the government or the law to review and assess a government department's operations. The audit objectives are to ensure that systems under development successfully meet the organisation's aims and objectives. From its audit work, the SAI comes to conclusions and issues reports about:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

More detailed objectives vary from audit scope, such as:

- Whether information systems sufficiently meet the business needs of the organisation
- Whether adequate controls and audit facilities have been built into the system

Auditors should communicate with the project sponsor about:

- The objectives of the review;
- Scope of the review in terms of SDLC stages to be covered by the review;
- Type of review –whether it is a pre-implementation review of the proposed SDLC, a parallel/concurrent review as SDLC stages are being executed, or a post-implementation review after the SDLC stages in question are completed;
- The timeframe of the review – the start dates and the end dates;
- Processes for reporting observations and recommendations;
- Process for following up on the agreed actions.

Collect the background information

As well as information gathered at the planning stage, auditors should obtain detailed information of the organisation and the environment in which it operates to perform the control review. A vital part of gaining this information is to gather information about the organisation's IT systems. Without such information, the auditors would be unable to say that a full understanding of the organisation has been achieved.

Typically, gaining information about the organisation's IT systems will include gathering information on several aspects of the organisation's systems. This information will allow the auditors to make an assessment of the complexity of the systems to be reviewed. This will in turn have an impact on the skills and resources required to carry out the review.

The information gathered by the auditors should include:

- Key documents: the IT strategy, the business plan and expenditure profiles.
- The hardware used to run its financial systems;
- System software (operating system, utilities, security software and networking software);
- Financial and other applications: auditors should determine which applications are to be reviewed as part of the audit process;
- Key organisation staff in both the finance and IT departments. When carrying out a detailed control review, IT auditors need to contact and interview these staff.

IT auditors will also need to know:

- Whether there have been any problems with the organisation's IT systems. For example, in previous years the organisation's system may have been unable to produce a complete trial balance;

- What changes, if any, are planned for the IT system;
- Are there any written policy or detailed management practices to govern systems development projects?
- Is there a management steering committee? Who is assigned specific responsibilities for systems development projects?
- Is there an appropriate systems development methodology which provides for periodic milestone events?
- Is there a project management and control system which requires preparation of time and cost budgets and then measurement of actual vs. planned results?
- Is there an independent quality assurance function which monitors the details of systems development projects?
- Is a project manager assigned with overall responsibility for direction and coordination of systems development?
- Are adequate standards for complex systems development used?
- Do documentation standards provide detailed guidance for each step and each product during systems development?
- Is there a comprehensive data security function which monitors systems development, maintenance and operation?
- Is there a comprehensive data administration function and have detailed responsibilities and authority been established?
- Is there a comprehensive data dictionary and is it required during systems development and modification?
- Are feasibility, impact, cost/benefit, and risk analyses prepared, approved and maintained during systems development projects?
- Are internal controls and security features included with systems design?
- Are the internal auditors required to monitor systems development projects, sign-off at milestones and review and approve acceptance test results?

All this information could describe the existing information systems and technology, identify available resources, and define known problems. It could be collected in such ways as:

- Previous working papers: auditors should confirm that the information remains up to date and accurate;
- Observation: touring the organisation's IT facilities;
- Interviewing IT personnel;
- Reviewing internal audit reports.

Assess materiality, identify the software to be audited

In a single IT Audit project, auditors clearly get audit objectives and scope from the project sponsor. In this case, it is not a question to identify which systems development cycle should be audited.

When review work is one part of a financial audit project, auditors need to identify the application software to be audited and ascertain the audit scope, because organisations always have many applications for different departments or businesses. In this case, the value of the assets controlled by the system(s) or the value of transactions processed per day/week/month/year should be considered when assessing materiality.

Identify the software life cycle

Adopting a suitable SDLC is important for developing project management. Each organisation should establish a SDLC methodology and assign responsibility for each phase of the cycle so that system design, development, and maintenance may progress smoothly and accurately. This cycle starts with a perceived need and extends through feasibility study, design and development, testing, implementation, system acceptance and approval, post-implementation review, and maintenance of the application and systems software. Following each phase of this cycle ensures that the new or revised software meets the organisation's needs, that adequate internal controls are consistent with management's objectives, and that the application is properly implemented. The method can be adjusted to comply with project requirements. Auditors should interview the project managers and clarify the SDLC and detailed process.

Identify the controls adopted in SDLC

Auditors should ask the management what risks had been identified and what control actions had been adopted in each stage of the SDLC. At the same time the auditor can perform some non-sampling control tests.

Auditors should prepare a control list of each stage for reviewing work. The detailed control actions list will be set out as follows.

SDLC Methodology

1. Determine the extent of the responsibilities of management, internal audit, users, quality assurance, and data processing during the system design, development, and maintenance.
2. Review SDLC work papers to determine if the appropriate levels of authorisation were obtained for each phase.

Requirement Analysis

3. Review and evaluate the procedures for performing a requirement analysis.
4. Review requirement analysis for a recent project and determine if it conforms to standards.

Systems Design and Development

5. Review and evaluate the procedures for systems design and development.
6. Review design specifications schedules, look for written evidence of approval, and determine if the design specifications comply with the standards.
7. Determine if an audit trail and programmed controls are incorporated in the design specifications of a recent project.
8. Review samples of source documents used for data entry, which are included in SDLC working papers of a recently developed application. Determine if they are designed to facilitate accurate gathering and entry of information.
9. Obtain and review programs to determine if they comply with the organisation's programming standards.

Testing Procedures

10. Review and evaluate the procedures for system and program testing.
11. Review documented testing procedures, test data, and resulting output to determine if they appear to be comprehensive and if they follow the organisation's standards.
12. Review the adequacy of tests.

Implementation Procedures

13. Review and evaluate procedures for program promotion and implementation.
14. Review documentation of the program promotion procedure. Determine if the standards are followed. Trace selected program and system software changes to the appropriate supporting records to determine if the changes have been properly approved.
15. Review documentation of the conversion/implementation of a newly developed application. Determine if the organisation's implementation procedures were followed.

Post-implementation Review

16. Review and evaluate the procedures for performing post-implementation reviews.
17. Review program modifications, testing procedures, and the preparation of supporting documentation to determine if the organisation's standards are being followed.

Maintenance of Applications

18. Review and evaluate the procedures for the maintenance of existing applications.

Preliminarily assess whether controls are in effect

Based on the evaluation of information system developing controls and results of non-sampling control tests, the auditors should preliminarily assess the effectiveness of the controls by doing the following checks:

- Review and evaluate the procedures for modifying systems software.
- Review systems software modifications, testing procedures, and the preparation of supporting documentation to determine if the organisation's standards are being followed.
- Review and evaluate documentation of in-house developed systems software and the features/options of proprietary systems software in use.For each significant assertion in each significant account, the auditors should assess control risks at one of the following three levels:
- Low control risks: The auditors believe that controls will prevent or detect any aggregate misstatements that could occur in the assertion in excess of design materiality.
- Moderate control risks: The auditors believe that controls will be in effect, but not enough to prevent or detect all aggregate misstatements that could occur in the assertion in excess of design materiality.
- High control risks: The auditors believe that controls have essential defects and are unlikely to prevent or detect any aggregate misstatements that could occur in the assertion in excess of design materiality.

During the check, the auditors should obtain sufficient:

- Information to develop comments in the auditors ' report or management letter and;
- Evidence to support the preliminary assessment of the effectiveness of internal controls.

Confirm the audit method

Auditors can collect evidence by using methods such as interviews, questionnaires, tour of business, and review of documents. Auditors can also use computer aided audit technique and tools (CAATTs) to examine the data flows such as snapshot, tracing, mapping, or verifying data and file integrity with Parallel Simulation, Test Data and Integrated Test Facilities.

2. Audit Implementation

Project initiation

A project is a management environment set up to deliver a business product to a specified business case. The aim of Project Initiation is to undertake the groundwork for the future management of a project and to obtain authority for it to proceed. Depending on the scale of the project, Initiation might relate to a study (e.g. a Feasibility Study), to the entire project, or to a single stage of a project (e.g. the Technical Design stage).An initiation stage might therefore occur at a number of points in the SDLC.

Definite financial authority is normally needed before the Initiation Stage is reached. The level of authority necessary to approve the expenditure will generally depend on the value of the project, the organisation's rules and delegated financial approval.

The results of this work should be presented to the approving authority (e.g. the IT Steering Committee) in a formal report, i.e. the Project Initiation Document ("PID"), for them to consider and authorise. The PID should include the details of:

- Legislative and/or business needs;
- Project objectives and time-scales;
- Management, organisation (Project Board, Project Manager, Stage Manager and the Quality Assurance Team);
- The scope of the project;
- Major control points for all stages of the project;
- All project deliverables;
- Technical and resource plans in sufficient details to calculate and allocate staff, costs and resources for the project;
- Quality criteria;
- Risks to successful completion, and proposed ways of managing identified risks;
- Any training needs which must be satisfied before the project commences;
- Any options raised in earlier reports (e.g. The Feasibility Study Report);
- Continuing validity of the existing user requirements, and of any assumptions and recommendations;
- The identification and management of both business and security risks;
- Any need to sustain or improve the level of service with limited or reduced staff numbers;
- Obsolescence of existing hardware, software or communications.

Audit considerations

The purpose of the project, and its scale, should be taken into account when deciding exactly what needs to be reviewed at this stage of the SDLC. Generally speaking, the following factors should be considered:

- Has an appropriate authorising authority given formal approval for the project to proceed?
- When approving the project, were adequate alternative options considered during the Feasibility Study and presented to the approving authority?
- Was each option evaluated in terms of its business benefits, costs and strategic fit?
- Are the estimates of business benefits achievable and measurable, and have workable methods for measuring achievement been defined?
- Does the Business Case include the costs of staff training and of developing a Business Continuity Plan?
- Is the estimated pay-back period longer than the likely economic working life of the system?
- Does the viability of the Business Case rely heavily on long term estimates? (the risks associated with long term measurement periods need to be included in the project risk assessment)
- Does the cost/benefit analysis include appropriate tolerance (e.g. 10%) to take account of under-estimates of costs and over-estimates of benefits?
- Have project risks been identified, measured and considered by the approving authority?
- Does the project clearly link with the existing or future business needs?
- Does the project clearly define:
  - The end product(s) to be produced at each stage of the project?
  - Time-scales and deadlines project stages?
  - Budgets and resource allocations for each project stage?
  - Project organisation and responsibilities?
  - Arrangements for monitoring and reporting progress?
  - The quality assurance criteria to be applied at each stage of the project?
  - Arrangements for assessing risks to the successful completion of the project as it progresses?
- Has a full time and experienced Project Manager been appointed to manage the project?
- Do project management standards specify the stages at which products are to be produced and progress reviews to take place?

Feasibility study

The Feasibility Study Report is the end product of the Feasibility Study. The main objective of a Feasibility Study Report is to determine whether a proposal is viable and to recommend suitable action where necessary. The study might be undertaken by the organisation's own staff (from both the IT Department and the end users), by external consultants, or a mixture of both. The study recommends the best way forward and it will:

- Define the problems or needs that require solution;
- Define broad or major requirements of the required solution;
- Determine if a computerised solution is required or desired;
- Determine if an existing system can be enhanced to correct the situation;
- Determine if a commercial product offers a solution to the problem;
- For each alternative, provide the estimate of costs, benefits, technical and business risk, time-scales, and an assessment of the option's 'fit' or compliance with the organisation's IT Strategy.
- Identify a suitable solution to the problem, and seek authority to proceed with its development;
- Recommend developing or acquiring a demonstration system.

Audit considerations

This is an analysis of the possibility and worthiness of undertaking the project and determining whether a proposal is viable and to recommend a suitable action. Auditors should check:

- Is the feasibility analysis well documented and clear?
- Have departments involved in systems development and operation been consulted during the feasibility analysis and have their recommendations been included?
- Does the feasibility analysis reflect any significant differences from original objectives, boundaries, and interfaces?
- Is the preliminary design in sufficient detail to support time and cost estimates, cost/benefit analysis, and impact study adequately?
- Does the preliminary design meet user requirements?
- Does the preliminary design reflect corporate standards?
- Has the project plan been prepared?
- Are the conclusions and recommendations supported by the feasibility analysis?
- Do the recommendations conform with corporate policies and practices?
- Has the feasibility analysis report been submitted to the management steering committee for action?
- Have responsible departments signed off the feasibility phase?
- Have the internal auditors prepared a milestone report with opinions and recommendations for the feasibility analysis phase?

Project planning

Project Planning outline plans for the reminder of the project including time-scale for implementation, and the proposed management structure for project development and implementation.

In the Project Initiation phase, systems are planned using a strategic approach. Executives and others evaluate the effectiveness of systems in terms of meeting the entity's mission and objectives. This process includes general guidelines for system selection and systems budgeting. Management develops a written long-term plan for systems that is strategic in nature. The plan will change in a few months, but much evidence exists that such planning is conducive to achieving effective IT solutions over the long term.

During this phase, several documents will be generated. They include the long-term plan, policies for selection of IT projects, and a long-term and short-term IT budget, as well as preliminary feasibility studies and project authorisations. Project proposals should have been documented when submitted to management, and a project schedule should exist that contains the approved projects.

The presence of these documents illustrates a structured, formal approach to systems development and, as such, illustrates an effective planning system for IT projects and systems. It also demonstrates a formal manner of approving IT projects.

IT auditors will verify the presence of the systems planning phase and take samples of the documents to verify the effectiveness of that system. The same audit procedures will be true for all of the other seven phases and, therefore, will not be repeated in the narratives of other phases.

Audit considerations

The purpose of this step is to determine if the project team has established a project plan and if the project plan was followed and any deviations documented, including extensions of the schedule. Auditors should check:

- Is the plan documented?
- Do the time frames appear realistic?
- Are the critical phases determined?
- Does the plan require management/user approval at specified points?
- Can the project be cancelled at the earliest points?
- Determine if the project plan included all the required phases of project development, including test phase, training for users, conversion, and implementation.
- Does it cover all applications and areas concerned?
- Does it cover all interfaces to/from the application?

User Requirement Analysis

The purpose of this step is to understand the existing system and determine the users' information and performance requirements. In this phase, IT professionals gather information requirements for the IT project. Facts and samples to be used in the IT project are gathered primarily from end users. A system analyst or developer then processes the requirements, producing a document, the User Requirement Specification (URS), which summarises the analysis of the IT project.

The URS is about "getting what you want", written in non-technical terms and consolidating all the materials produced to date relating to the business functions of the required system. It is a detailed statement of users' requirements and provides a basis for design work, suppliers to submit proposals and acceptance testing criteria. A good specification should be "ACCURATE": accurate, clear, concise, unambiguous, relevant, adequate, thorough and effective.User Requirement Specifications describe the:

- Organisation's business;
- Formal declaration of the users' requirements of the proposed system;
- Existing system (incl. deficiencies);
- Objectives of the proposed system;
- Required functions (mandatory and optional);
- Expected performance;
- Constraints (e.g. environment, accommodation, locations of staff);
- Project timetable;
- Facilities required;
- IT security;
- Acceptance testing criteria;
- Documentation;
- Training;
- Maintenance.

If a decision has been made to buy a system (or indeed a service such as facilities management), the URS should be sufficiently comprehensive to form the basis for advising potential suppliers in full of the organisation's needs, and enable them to respond with detailed proposals of how they propose to satisfy those needs. As a rule, the URS should therefore be written in such a way that it does not constrain the options open to either designers or prospective suppliers to provide innovative solutions by specifying exactly what technical solutions are to be employed in meeting the users' requirements.

It is important to ensure that the system's final owner 'signs off' the User Requirement Specification to signify understanding and agreement before the project proceeds further.

Audit considerations

- Efficiency
- Effectiveness
- Are user requirements well documented and clear?
- Is the responsible user executive specified?
- Have the user executives approved the requirements?
- Is a priority for implementation requested?
- Is the project included in the long- or short-range systems plan?
- Are the business objectives expressed clearly?
- Is the scope of the project defined well?
- Are claimed benefits supported?
- Is a solution or solutions to business objectives proposed?
- Are there necessary audit functions included in the new system?
- Does the requirements study include potential needs for the future?
- Does the requirements study consider potential use in meeting common needs?
- Are existing systems to be replaced or interfaced identified clearly?
- Are existing systems to be replaced or interfaced documented adequately and accurately?
- Is the new system compatible with other applications / systems?
- Could the new system recover after failure?
- Have other departments involved in systems development and operation been consulted during preparation of the requirements and have recommendations been included?
- Do user requirements include security, controls and privacy measures?
- Do benefits claimed appear to be reasonable?
- Do user requirements appear to reflect actual needs?
- Are effective change and version control procedures in place?
- Does the procurement procedure help to ensure the organisation obtain good VFM?

Purchased software or systems development

When an organisation plans to use some kinds of software, it should make a decision to purchase on the open market or have it developed by its own programmers. Software products purchased on the open market are often credible and tested precisely, but not specialised for the organisation. Although applications developed by its own programmers are mostly suitable for organisation, the applications are likely to have security vulnerabilities and hidden failures. So both situations should be audited.

Purchased software

This topic may include the procurement process. Purchased software packages should be compatible with existing IT function operations, meet the requirements of the users and should be reliable enough to work satisfactorily under operational workloads and conditions. Software product acquisition procedures should follow the organisation policies, and these products should be tested and reviewed before they are used and paid for.

Audit considerations

- Are there vendor evaluation criteria?
- Are there invitation procedures for bidding?
- Are there selection procedures for vendor?
- Does the contract provide for product requirements as stated or modified by the organisation?
- Does the vender warrant that the product will perform as specified in the contract?
- Does the contract indicate how performance of those product specifications will be measured?
- Does the vender warrant that the product will meet the requirements in the organisation's operating environment?
- Does the contract specify on what date the product will be operational?
- Does the contract indicate the level of performance for the product?
- Does the contract provide for remedy to the organisation when the product fails to achieve the performance level?
- Does the contract provide for a system of controls(Security Controls, Audit trail features, Passwords Controls, etc) sufficient to detect reliability concerns?
- Does the software provide for sufficient data validation routines to detect input errors?
- Does the contract provide for adequate controls to detect the loss of file integrity?
- Does the contract provide for adequate backup and recovery controls?
- Does the vendor provide manuals for systems analysts and programmers to understand the application?
- Are the operator manuals included in the contract?
- Does the contract provide for the specified user manuals?
- Does the contract provide for documentation to assist organisation personnel in tracking down and correcting problems?
- Does the contract specify the costs associated with performing maintenance?
- Is the length of maintenance warranty periods specified in the contract?
- Does the organisation have the right to have maintenance performed by other than the vendor?
- Have provisions been made for vendor personnel to access to restricted areas to perform maintenance?
- Does the vendor require communication access to a vendor computer to perform maintenance?
- Does the contract provide for needed hardware upgrades?
- Does the contract provide for upgrading the application software in accordance with operating system upgrades?
- Does the contract provide how the user will request changes to software?
- Does the contract provide for the costs of enhancing the software at later dates?
- Has the vendor selection process been fair?
- Is the contract such that it would encourage the vendor to complete the contract?
- Does the selected vendor have a high probability of being in business during the duration of the contract?
- Have penalties been established in case the vendor fails to meet the contractual requirements?
- Do the terms of the contract conform to the organisation's contractual term requirements?
- If the contract is terminated, have the termination provisions been specified?

- If the contract is a lease contract, does it provide for part of that lease being applicable to a purchase?
- Can the organisation terminate the contract at any time?
- Does the contract specify the state or country whose laws govern the contract?
- Does the vendor provide for operator training?
- Is the location of training specified in the contract?
- Does the contract provide for training of data processing personnel in the use of the application?
- Does the contract provide for training of user personnel in preparing input and using system outputs?
- Can user personnel be reasonably expected to prepare the application input accurately and completely?
- Are the reports and manuals designed for the skill levels present in the organisation?
- Can the software be moved from the current hardware to the next most logical piece of hardware?
- Will the vendor continue support for a reasonable period of time?

Systems development

Systems development process is the translation of users' needs or goals into software products. The developed software should meet organisation users' expectation and run steady. The systems development process comprises several stages, including specifying user requirements, general design, detailed design, systems development, development testing, acceptance and so on.

Systems Requirement Specifications

Once the user requirement specifications have been approved, the project team starts designing the new system. The system design is meant to be a blueprint of the new IT system. The project team considers and evaluates alternative designs and selects the one that is expected to meet the user requirements most satisfactorily within the given constraints. Specifying user requirements encompasses those tasks that go into determining the needs or conditions to be met for a new or altered product, taking account of the possibly conflicting requirements of the various stakeholders. The output of this stage is the system design document (SDD). The SDD is submitted to top management for approval. The SDD includes the following:

- Data flow in the information system;
- Database structure;
- Hardware and software configurations;
- User interface: That is, how the users are expected to interact with the system;
- Physical facilities required.

Audit considerations

- Are systems specifications documented well and clearly?
- Have significant changes to systems design been controlled and approved by cognisant authority?
- Has a detailed work plan been prepared for the systems specifications phase?
- Has the systems development methodology been used effectively during development of systems specifications?
- Has the project management and control system been used effectively?
- Has actual accomplishment during development of systems specifications been reasonably close to estimates?
- Are systems development team resources adequate to accomplish objectives?
- Have time and cost estimates, cost/benefit analysis, and impact study been updated?
- Have significant changes to project scope been approved by the management steering committee?
- Do systems specifications reflect accurately approved functional design features and user requirements?
- Is it reasonable to expect the systems specifications to be implemented satisfactorily within user and data processing environments?
- Do the systems specifications provide adequately for internal controls and data security?
- Do the systems specifications provide adequately for requested audit features?
- Has an appropriate configuration for hardware and software been selected for implementation of the systems design and specifications?
- Have the hardware and software selected been reviewed for adequacy of internal controls, data security, integrity, and dependability?
- Do systems specifications provide adequately for corporate standards and practices?
- Have systems acceptance criteria been updated?
- Has the systems test plan been updated?
- Has data administration reviewed systems specifications?
- Has data security reviewed systems specifications?
- Has quality assurance reviewed systems specifications?
- Has data processing operations reviewed systems specifications?
- Have user departments reviewed systems specifications?
- Has the risk analysis been updated?
- Have systems specifications been submitted to the management steering committee for action?
- Have responsible departments signed off the systems specifications?
- Have the internal auditors prepared a milestone report with opinions and recommendations for the systems specifications phase?

General design

Before coding and developing, an organisation should have specific software design, which encompasses general design and detailed design. Designers should produce one or more 'models' of what they see a system eventually looking like, with ideas from the analysis section either used or discarded. The general design translates requirement specifications to future software architecture.

Audit considerations

- Were users adequately consulted?
- Were alternative designs considered?
- Did the selected design meet the user requirement?
- Was an adequate financial audit trail provided?
- Were adequate controls provided?
- Was the design flexible enough to cope with change?
- Were hardware and software configurations specified?
- Did system security designs meet user needs?
- Did users sign off the system design?

Detailed design

Detailed design is the step where the software documentation is prepared for coding. In this stage, the organisation should prepare detailed design and technical software application requirements and define the criteria for acceptance of the requirements. The organisation should have the requirements approved to ensure that they correspond to the high-level design and perform reassessment when significant technical or logical discrepancies occur during development or maintenance. They should consider the confidentiality, integrity and availability of the system.

Audit considerations

- Is the systems design well documented and clear?
- Have significant changes to the preliminary design been controlled and approved by cognisant authority?
- Has a detailed work plan been prepared for the design phase?
- Has the systems development methodology(structured design techniques, prototyping, etc) been used effectively?

- Has the project management and control system been used effectively?
- Has actual accomplishment been reasonably close to estimates?
- Are systems development team resources adequate to accomplish objectives?
- Have time and cost estimates, cost/benefit analysis, and impact study been updated?
- Have significant changes to project scope been approved by the management steering committee?
- Do detailed functional design features accurately reflect approved detailed user requirements?
- Is it reasonable to expect the designed system to be implemented satisfactorily within the user and data processing environments?
- Does the design provide adequately for internal controls and data security?
- Does the design provide adequately for requested audit features?
- Have the requirements for hardware and systems software been developed and can they be met satisfactorily with resources available or approved for installation?
- Does the design provide adequately for corporate standards and practices?
- Have systems design acceptance criteria been prepared?
- Has the systems test plan been prepared?
- Does the design provide adequately for incident management(offsite backup and recovery measures, etc)?
- Does the design provide adequately for capacity management?
- Has data administration reviewed the systems design?
- Has data security reviewed the systems design?
- Has quality assurance reviewed the systems design?
- Has data processing operations reviewed the systems design?
- Have cognisant user departments reviewed the systems design?
- Has a risk analysis been conducted?
- Is the input defined in detail?
- Is the output defined in detail?
- Is the functional logic defined in detail?
- Is the logical file structure defined in detail?
- Has the systems design been submitted to the management steering committee for action?
- Have responsible departments signed off the systems design?
- Have the internal auditors prepared a milestone report with opinions and recommendations for the design phase?

Systems development

Systems development transfers the design onto the physical system by building the technical architecture and purchasing the material needed to build the system and building the database and programs. IT specialists write programs which will be used on the system.

There are several kinds of development methodology used in systems development, such as: Data-Oriented Development, Object-Oriented Development, Component-Based Development, Web-Based Development, Prototyping, Rapid Development and Agile Development.

The audit may consider the usage of program coding standards. These standards enhance the quality of programming activities and future maintenance capabilities.

Audit considerations

- Has a detailed work plan been prepared for the systems development phase?
- Has the systems development methodology been used effectively during the systems development phase?
- Is the methodology used for systems development appropriate?
- Has the project management and control system(version control, incident/problem management capability, etc) been used effectively during the systems development phase?
- Has actual accomplishment during systems development been reasonably close to estimates?
- Have significant changes to systems specifications been controlled and approved by cognisant authority?
- Are systems development team resources adequate to accomplish objectives of systems development phase?
- Have time and cost estimates, cost/benefit analysis, impact study, and risk analysis been updated?
- Have significant changes to project scope been approved by the management steering committee?
- Are there version controls during systems phase?
- Is there incident/problem management capability?
- Do program specifications and user procedures accurately reflect approved systems specifications?
- Do program specifications and user procedures provide adequately for internal controls and data security?
- Do program specifications and user procedures provide adequately for requested audit features?
- Are data elements, including interfacing data sets, entered in the data dictionary?
- Have procedures and/or programs been developed and documented for loading data files, initialising data files, systems conversion, year end processing, onsite backup and recovery, offsite backup and recovery?
- Is there a detailed, written training plan?
- Is there a detailed, written test plan, including Unit test, Integrated test, Systems test, Pilot test, Acceptance test, Parallel test?
- Has a test coordinator been assigned?
- Are tests documented well?
- Have all tests been reviewed in detail by at least one level?
- Have the test results been reviewed by the internal auditors and are they satisfied?
- Do products of the systems development phase conform with corporate standards and practices?
- Have products of the systems development phase been submitted to the management steering committee for action?
- Have responsible departments signed off products of the systems development phase?
- Have the internal auditors prepared a milestone report with opinions and recommendations for the systems development phase?

Development testing

Development testing generally comprises unit testing and integration testing. Unit testing is the testing of an individual program module in an isolated environment before combining it with other modules to form a program. The objective is to determine whether the module is capable of accepting specific input and producing the correct outputs. The programming team leader normally carries out unit testing. Program testing follows similar objectives, but with all the modules in place to form a complete program. Integration testing is the process of adding new programs to an evolving system. Testing needs to find errors in the interfaces between programs, the discrepancies between the program functions performed and those specified and those unspecified functions are performed.

Meanwhile, development testing may be elaborated in more detail, specifically with regard to:

- Recovery Testing
- Security Testing
- Stress Testing
- Volume Testing
- Performance Testing

Audit considerations

- Determine if the system is adequately tested prior to implementation, the test plan includes all aspects of the new system, and all unexpected results are thoroughly resolved. Has the test plan been documented, including:
  - Unit test;
  - Integrated test;
  - System test including interfaces;
  - Pilot test;
  - Parallel test.
- Are the users included in the testing?
- Has testing been done at a proper testing facility?
- Testing of system functionalities requested by the audit function at user requirements and design stages.
- Has software scanning been done to see if any unnecessary code resides?
- Do the users have to sign-off on the success of the test programme?
- Are all aspects of the system tested, as outlined in the detail requirements?
- Have the system results been reviewed in detail?
- Is there a problem resolution procedure for those tests not meeting the expected results?

Acceptance

Acceptance is based on an analysis of the User Requirement Specification and any other acceptance criteria defined during design and development. The aim is to identify that requirements, facilities and functions should be tested, their relative importance, and the method of testing to be adopted for each. During acceptance, user acceptance testing and quality acceptance testing are good methods.

Audit considerations

- Are the results of the test plan satisfactory?
- Has data processing operations conducted a systems turnover evaluation and is the result satisfactory?
- Is the system documented adequately?
- Has an internal controls review been made?
- Is the level of internal controls satisfactory?
- Are the results of the parallel test satisfactory?
- Is the result of the test of backup and recovery tests satisfactory?
- Have responsible departments approved the system for implementation?
- Has the management steering committee approved the system for implementation?
- Have the internal auditors prepared a milestone report with opinions and recommendations for systems implementation?

Parallel running, post-implementation review and maintenance

Post Implementation Review (PIR) is the final stage of a system development project. Its aim is to establish the degree of success achieved by the development project, and whether any lessons can be applied to improving the organisation's development process. Meanwhile, parallel running and maintenance all should be taken into account. Auditors should pay attention to the adequacy of the system in meeting user requirements and evaluation of cost benefits or return on investment measurements.

Audit considerations

- Has all relevant data been transferred to the new system in a controlled manner?
- Which changeover approach has been used? Parallel changeover, phased changeover or abrupt changeover?
- Are backup and recovery procedures documented, and have they been tested?
- Has the training programme been completed? Has any attempt been made to measure its effectiveness?
- Are user manuals clear, unambiguous and easy to understand? Do they incorporate all late changes to the system?
- Have responsibilities been assigned for carrying out clerical procedures and controls, and have they been tested?
- Has a System Administrator been appointed and trained? Are system administration activities documented?
- Has a documented plan been produced for reverting to the existing system should the need arise? Is it workable?
- Is there a system security policy? Has it been approved by the System Owner?
- Is it commensurate with the corporate IT Security Policy? Does it address all relevant risks?
- Has it been implemented?
- Has a documented business continuity plan been produced? Has it been tested?
- Are documented change and configuration management procedures in place?
- Has a monitoring process been established to determine the efficacy of the system?
- Has the system proved stable since go-live?
- Is a service level agreement in place for the system?
- Have all parties been satisfied with the level of service to date?
- Has the system integrated effectively with other systems?
- Has vendor support been adequate, effective and timely?
- Has security within the system been effective?
- If the system has been a joint effort between two or more vendors, have they worked effectively together?

Configuration management and change management

Configuration and change management help ensure an orderly process for the control of changes to project baseline products as they evolve through each project phase.

Audit considerations

- Are there any procedures and policies related to change management?
- Have all changes from the original specification been properly identified, assessed/evaluated, reviewed, and implemented, tested, and logged and authorised?
- Have all changes to the application since go-live been logged and authorised?
- Have all changes before and after the implementation been tested?
- Have all changes been documented?
- Are changes which require more than a specified level of resource, or which are likely to cause significant slippage in the project timetable, referred to the Project Board for approval?
- Have all changes been reviewed for compliance with change and configuration management procedures, and authorised for release?

Segregation of duty

In a manual system, separate persons should be responsible for initiating transactions, recording transactions, and maintaining custody of assets. As a basic control, segregation of duty prevents or detects errors and irregularities. In an IT system, however, the traditional notion of segregation of duties does not always apply, because the program is performing functions that in a manual system would be considered to be incompatible. So segregation of duties must exist in a different form.

Audit considerations

- Is there clear segregation of duties among those who build, test and operate the system?
- Is there an implemented practice in the IT function to ensure that roles and responsibilities are properly exercised?
- Do all personnel have sufficient authority and resources to execute their roles and responsibilities?
- Does the management make sure that personnel are performing only authorised duties relevant to their respective jobs and positions?

Operation management

Input controls

Input controls are to ensure the authenticity, accuracy, completeness, and timeliness of data entered in to the system. A manual or operating procedure should exist for system users.

Audit considerations

- Transactions are from recognised sources. Determine the audit trail for documents prior to input to an application.
- Follow through a document to check that controls ensure input is only accepted from recognised sources. E.g. a valid timesheet.
- Transactions are explicitly authorised by either manual or electronic means.
- Establish how input is authorised.
- Request a list of all users of the system from the Systems Administrator. Ensure that all system users are valid employees and users.
- Password controls should be effective in restricting access.
- Ensure that access to the system requires a unique ID and password. Ideally the password should be alphanumeric and changed periodically.
- Input and authorisation functions are restricted and separated.
    - Is there an effective segregation of duties to prevent authorising transactions and vice versa?
    - Can the system produce a system security report, which includes user access permissions?
- Input of parameters for processing and other standing data is strictly controlled
    - What controls exist to prevent accidental / malicious changes to fixed data parameters i.e. tax calculations, pay rise etc.
    - Check the correctness of key values and data within the system.
- Does the system record a history of standing data changes?
- Data should be subject to validation for completeness and accuracy at input stage
- Establish if key fields are validated, what the criteria is and who ensures this is carried out.
- There should be clear procedures for data items rejected on input.
- Ascertain how rejected inputs are treated and reported. From samples of rejected records, ensure that they are amended and successfully re-input.
- Clear timetables should exist for input and should be adhered to.
- Ascertain who is responsible for authorising the processing of jobs and what procedures are in place.
- Are they reviewed on a regular basis?
- Checks should be made to detect possible duplicate input records. Determine what checks for duplicate input are carried out by the application itself, and how they are reported / followed up.
- Determine the action taken and the reason for the duplicates arising.

Processing controls

Processing controls should ensure the project meets the objectives defined in the original proposal.

Audit considerations

- Were the expected benefits of the new system realised?
- Does the system perform as expected?
- If there were differences found between expected and actual results, were they investigated?
- If there were inefficiencies noted, were they documented?
- Are transactions and account balances properly recorded on the Accounting systems, if applicable? (What accounts will the transactions affect?).
- Have written procedures been prepared that explain all error codes and messages, and corrective action for each?
- Does the application have provisions that prevent concurrent file/record updates?
- Is the file/record locked when one user is accessing in update, and are appropriate error messages provided?
- Does the application have controls to check for data integrity?
- Can the system-generated transactions be traced back to the source for reconciliation?
- Are there adequate audit trails for tracing purposes?

Output controls

If output data has been classified according to the Security Policy/Plan, information can be classified as restricted, confidential, public, etc. Output controls should ensure that the processing of stored information is correct and appropriate to circumstances.

Audit considerations

- Is there detail documentation for output requirements? (Output includes reports as well as files.)
- Are all departments' concerns considered?
- Does the documentation include as follows:
    - Who is to receive the reports?
    - Retention of reports and files, and
    - Is the audit trail sufficient to identify who, when, how and why a user accessed a resource or amended an item?
- Does the output provide the users with the ability to control and ensure the completeness, accuracy, and authorisation of the data?
- Do the reports include the ability to trace the originator of each transaction?
- Do the reports include control totals, if applicable?
- Is there a means to verify the information included on the reports?
- Have the routing and distribution procedures been established?

Maintenance management

The help desk management

The help desk should make a quick response to a user's problem, transfer or deal with it quickly, so the problem will have least effect on the system running. Furthermore, it should analyse the problem and find out the reason, and then classify the problem and provide the support for other work.

Audit considerations

- Whether the help desk can response to users' problems, transfer or deal with them quickly, so the problems will have least effect on the system running;
- Whether the help desk can analyse the problems and find out the reasons;
- Whether the help desk can classify the problems and provide the support for other work.

Are logs periodically checked?

Auditors should check:

- Does the application have the capability to successfully perform logging?
- Have all failed logon attempts been logged?
- Are all sensitive transactions and changes logged and an audit trail created?
- Does the audit trail contain who made the change, when it was made, and what was changed?
- Is the system administrator the only one who has access to change or delete these logs or audit trails?

Is there is periodic check on the application?

Auditors should check:

- Have the processes and tools used to report, track, approve, fix, and monitor changes on the application been determined?
- Does the code reside in a code library or a different tool when being changed?
- Has the access to the code library been restricted?
- Have all requests for change been reviewed and authorised?
- Have all completed changes been reviewed for compliance with change and configuration management procedures, and authorised for release?

Security management

Physical security

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Controls should be adopted to minimise the risk from potential threats such as water, electrical supply, fire, etc.

Audit considerations

- Are items secured in some way?
- Are terminals in a locked, inaccessible area, kept away from the public and unauthorised users?
- Are there controls over the modems?
- Are diskettes stored in fireproof cabinet?
- Are backups stored off site?
- Are backup materials stored in a secure tape library?

Logical security

Logical Security consists of software safeguards for an organisation's systems, including user ID and password access, authentication, access rights and authority levels. These measures are to ensure that only authorised users are able to perform actions or access information in a network or a workstation.

Audit considerations

- Are there varying levels of security access for different types of transactions:
  - Inquiry only,
  - update non-monetary transactions,
  - update financial transactions, and
  - add/delete records.
- Are the levels appropriately assigned to the user department staff?
- Who has the ability to change passwords?
- Does the user department or data security control the password assignments?
- If controlled by the user department, does the staff member also have authority to input transactions?
- Are passwords masked, encrypted, stored in a visible file?
- Are there controls to log and monitor all sign-on attempts, both valid and invalid?
- Is all access to the system monitored?
- Does the application have controls in place to prevent unauthorised access to the system?
- Does the system lock out after a certain number of invalid sign-on attempts?
- Are both a password and logon-id required for access to the system?
- Are there controls against modern threats such as Viruses, Trojan Horses, Worms, Logic Bombs, Denial of Service attacks etc?

Audit Trail Reports

Auditors should determine if there are adequate and effective audit trails and reports designed in the system:

- Are detailed audit trail reports produced by the system automatically?
- Are audit reports listed on the report distribution schedule?
- Are the user departments satisfied with the information produced on the audit reports?
- Will the reports meet user and management needs?
- Will the reports satisfy audit needs?
- Can users input information, which will alter the audit trail reports?
- Are the reports distributed and reviewed by the appropriate people?

Data security

Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled.

Audit considerations

- Are different access levels, such as read only, update, delete and add, set to defend different data?
- Are different access levels set for different personnel?

Business continuity and disaster recovery

With the formidable challenges and the growing complexity of IT systems that support business operations, an organisation must make comprehensive managed efforts to prioritise key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organisational response to the challenges that surface during and after a crisis, which is called Business continuity planning. Disaster recovery involves an immediate intervention to minimise further losses brought on by a disaster and to begin the process of recovery, including activities and programmes designed to restore critical business functions and return the organisation to an acceptable condition.

Auditors should determine if there are adequate backup and recovery procedures developed for the system:

- Have procedures been developed for disaster recovery and restart for the system. Have the recovery/restart procedures been documented?
- Do the procedures include all foreseeable circumstances?
- Do the plans include recovery of hardware and software?
- Are there procedures for the periodic backup of the system?
- How often will backups be done?
- How long will the backups be kept?
- What media will the backups be done on? (Tape, disk, diskette)
- Have the backup procedures been documented?
- How will the backups be labelled?
- Is the labelling consistent?

Staff training

Insufficient training will increase the risk of the application being misused or the system interrupted. The organisation should make sure that its staff are well trained, and training materials are available and up to date.

Auditors should interview the development and user department leaders, talk about the training processes and get the latest training materials, user reference and other support materials.

To determine whether the IT staff and all users received a proper training prior implementation, auditors should review as follows:

- whether there is a detailed Training Manual, User Manual and Technical Manual.
- In case of outsourcing or in-house development, whether above manuals are produced by the end of the development activity and have been delivered by the application provider, whether manuals have been checked and signed off.
- In case of ready-made application, whether all different users received their manuals prior implementation.
- whether all manuals were reviewed and signed off.
- whether all common users had been trained before the deployment.
- whether Security Awareness Training has been included.
- whether there is special training for system maintenance staff and management.

3. Audit report

As a result of the auditing work, auditors should make a full report. Generally speaking, the report should include:

- **General descriptions:** In this section, auditors should state the audit objectives and scope, the methods used and the risk assessment.
- **Report of the audit findings and its impacts**: Auditors should state the detailed findings of control weakness and the substantial impacts.
- **Audit recommendations:** It is preferable that auditors give some recommendations for control weakness.

A standardised format for writing audit reports should at least include the following sections:

- **Executive Summary:** Restates conclusion(s) for each audit objective and summarises significant findings and recommendations.
- **Background:** Provides background information about the purpose/mission of the audited area. It should also indicate whether a follow-up on the previous audit is included or not.
- **Audit Objectives:** List all audit objectives.
- **Scope & Methodology:** Identifies audited activities, time period, and the nature and the extent of audit tests performed.
- **Audit Results:** This section should be restricted to the documented factual statements, which can be substantiated. Statements of opinion, assumption, and conclusion should be avoided.
- **Conclusions:** The auditors' opinion or conclusion based on the objectives of the audit should be stated.
- **Recommendations:** The auditors' recommendation based on the results of the audit should be stated. Each recommendation should be preceded by a discussion of the finding and followed by the management's response to the recommendation. If the management's response is too lengthy to be included in the body of the report, a summary of the response should be included in the report with the complete response attached to the report (i.e., Appendices).

Bibliography

1. The General Audit Guideline of the State Audit Bureau of Kuwait.
2. The High Tech Acquisitions Audit Manual of the State Audit Bureau of Kuwait.
3. COBIT 4.0
4. System Audit, M Revathy Sriram, Tata McGraw-Hill, 2001.
5. Managing The Audit Function, Michael P. Cangemi and Tommie Singleton, John Wiley & Sons, 2003.
6. Auditing Hardware and Software Contracts, William E. Perry, EDP Auditors Foundation.
7. www.adm.uwaterloo.ca
8. Post Implementation Reviews, David M. Burbage, 2001.
9. System Development Project, Judy Condon, 1999.
10. www.da.ks.gov
11. www.asosai.org
12. COBIT 4.1, IT governance institute, www.ISACA.org, 2007
13. Auditing Systems Development, INTOSAI IT AUDIT COMMITTEE, 2007
14. IT Audit Guidelines, 6th ASOSAI Research Project, 2003
15. Why IT projects fail, Steve Doughty, INTO IT 14, 2001
16. A new approach to the auditing of system development projects in South Africa, Eddie Pelcher, INTO IT 16, 2002
17. System Development Life Cycle (SDLC) Review, Document G23, www.isaca.org
18. System Development Life Cycle and IT Audits, Tommie W. Singleton, www.isaca.org, 2007
19. Chinese ITIL White paper, 2004

Glossary

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets. It usually is measured by a combination of impact and probability of occurrence.

SDLC: System development life cycle. The phases deployed in the development or acquisition of a software system. Typical phases include the feasibility study, requirements study, requirements definition, general design, detailed design, programming, testing, installation and post-implementation review.

SDD: System Design Document

CAATTs: computer aided audit techniques and tools

URS : User Requirement Specification, which summarises the analysis of the IT project.