ABC Financial System	Risk and Controls Assessment (sample only)						
Control Objective	**Existing & Planned Controls / Issues**	**L**	**C**	**LxC**	**Controls / Concerns**	**Residual Risk**	**Assessment/ Recommendation**
General Computer Controls:							
1 Access Controls Logical security procedures are established to ensure only authorized users, and IT support can access the system functions in accordance with their roles.	1.1 There are identification, authentication or access restrictions to provide security for the ABC System.	3	3	M	• Well documented, detailed logical security processes have been established. • Security architecture in place. • IDIR is used for authentication.	L	Control is adequate. No further recommendation.
	1.2 Users are assigned to systems and applications with appropriate limits on privileges.	3	3	M	• Access to the system is granted based on roles. • A client application administrator account is restricted to functions only associated with their own application (no view of data related to other applications).	L	Control is adequate. No further recommendation.
	1.3 Access privileges are approved by the system owner or delegate, and are not current.	4	3	H	• There is a formal access process, however user access requests and approval process not comprehensive and updated. • The plan is that accounts will be created based on application owner requests to the support group.	M	Control requires improvement. <u>Recommendation</u> Update the process and ensure it defines who is authorized to issue and approve requests, and how the request will be documented, stored and implemented.
2 Change Management Formal change management procedures are in place for application maintenance, and changes implanted do not jeopardize the security and integrity of the data.	2.1 A record is maintained of requests for program changes and their disposition.						
	2.2 There is assessment of the impact of changes.						
	2.3 There is a management trail of changes.						
	2.4 Changes are appropriately reviewed or authorized.						
	2.5 Users are involved in requirements testing, resulting in queries and/or functions that do not meet users' needs.						
	2.6 Control of changes (including logging of changes with audit trail, back-out processes, regarding changes and, rollbacks).						
3 Organization To ensure that defined functions, related resources and segregation of duties are established.	3.1 Ministry personnel are performing duties as they relate system changes that are appropriate for their job function.						
	3.2 Calculations are fully automated by the system requiring significant staff interaction.						
	3.3 Users are trained or aware of the changes applied to the application.						
	3.4 There are appropriate levels of staffing in terms of numbers and skill set to support the application, preventing the implementation of changes in due time.						
	3.5 Technical support staff do have adequate knowledge of the change requirements.						
4 Policy & Procedures To determine whether senior management has established and updated an adequate policy framework and related processes to accommodate the changes.	4.1 Ministry/Branch policy and procedures are updated and communicated to relevant stakeholders to reflect the related changes.						
	4.2 Policies and procedures do exist to control the activities of personnel leading to loss of data or damaged data.						
	4.3 There is technical / user manual for the application or it is current to reflect the changes.						

ABC Financial System	Risk and Controls Assessment (sample only)						
Control Objective	**Existing & Planned Controls / Issues**	**L**	**C**	**LxC**	**Controls / Concerns**	**Residual Risk**	**Assessment/ Recommendation**
Business Process Controls:							
5 Application Controls To ensure automated controls together with manual /procedural controls provide reasonable assurance that recorded transactions are processed in a valid, authorized, complete, accurate, and timely manner. To ensure control procedures are in place to provide reasonable assurance that the integrity of automated business rule drivers is established and maintained.	5.1 Creation, maintenance and use of record data is authorized and correct.						
	5.2 Approved invoices for integration with the CAS financial system are valid and accurate.						
	5.3 Expense Authority & Qualified Receiver & Revenue Authority roles and responsibilities have been clearly defined and articulated in training materials						
	5.4 Processes are in place to help ensure purchase invoice & or sales invoice data entry accuracy and completeness.						
	5.5 Processes are in place to ensure that invoice payments are not duplicated.						
	5.6 User Acceptance Testing (UAT) has confirmed that automated financial controls over invoice creation and approval are functioning as designed.						
	5.7 Additional oversight and monitoring functions in place to complement the overall control framework around transaction processing integrity.						
	5.8 The business rule definitions were done in close liaison with ministry program subject matter experts.						
	5.9 Business rules established in the system were an integral part of the User Acceptance Testing scripts/process.						
6 Interface to CAS Financials System To ensure whether information transmitted to CAS is recorded and processed completely and accurately in a timely manner.	6.1 Interface to CAS works properly.						
	6.2 Changes to the interface to CAS are tested, or test results are successful.						
	6.3 Monitoring and corrective action is taken on incomplete, inaccurate or invalid data sent to CAS.						
	6.4 Transactions that have been manually entered into CAS are also sent electronically by the application.						
	6.5 Valid accounting entries (e.g. bank account, suppliers, dates, etc) are sent to CAS.						
	6.6 Close periods are synchronized with CAS leading to reconciliation issues.						
7 Reconciliation to CAS Financials System To ensure that reconciliations are completely and accurately performed and exceptions cleared in a timely manner.	7.1 Reconciliation to CAS is done and completed in a timely manner.						
	7.2 Reconciliations are reviewed and approved.						
	7.3 Discrepancies identified by the reconciliation process are actioned.						
	7.4 Reconciliation reports are understandable and updated to reflect the implementation.						
	7.5 Staff are currently trained to resolve any reconciliation issues.						
	7.6 Ability to recover reconciliation reports.						

ABC Financial System	Risk and Controls Assessment (sample only)						
Control Objective	**Existing & Planned Controls / Issues**	**L**	**C**	**LxC**	**Controls / Concerns**	**Residual Risk**	**Assessment/ Recommendation**
8 Queries and Reports To ensure that applicable queries and reports are updated to accommodate the implementation.	8.1 Reports and queries are accurate & complete.						
	8.2 Reports and queries meet user and OCG needs.						
	8.3 Reports are run on a timely manner.						
	8.4 Exception reports are developed or updated requiring manual analysis.						
9 Management Trail / Compliance To ensure they exist, are reviewed, monitored and exceptions are followed up.	9.1 Management trail exists and is not disabled for financial data.						
	9.2 Logs (audit trails) are maintained for key fields or are retained for adequate periods.						
	9.3 Audit logs are reviewed and there is the ability to investigate inappropriate, unauthorized or out-of-the ordinary access and activities						
	9.4 Transactions are retained for a predetermined period, in accordance with retention requirements (Operational need, and legislation/regulation).						
	9.5 Creation, changes and deletion of/to critical and/or sensitive data elements are logged and periodically analyzed, as appropriate.						

L – is the likelihood of a risk occurring not considering any existing or planned controls, refer to Risk Ranking Tables.
C - is the consequence (or impact) should a risk event actually occur, refer to Risk Ranking Tables.
(LxC) - is the level of risk or inherent risk resulting from the relationship of L & C.
Residual Risk is the level remaining to mitigate the inherent risk after existing controls and the controls planned to be implemented.