Audit Programme for Business Process Re-engineering (BPR) Function

S/No.	Audit Entity	Test Procedures	Risk	Control	IS Security & Control Framework Reference
1	**Procedures and standard**	Determine if there is a standardized process improvement methodology in place.	Inconsistent practices and substandard operation by BPR developers.	Document procedures and standards for systems development.	
		Verify the mode of system development methodology in use.			
		Verify that in-house application development is performed in line with standard system development methods/life cycle.			
		Determine if there is a process of requesting for process automation from process owners to Business process automation & Re-engineering (BPR) unit. Either automated or manual.			
		Review the process of requesting for process automation from process owners to BPR unit to ensure that appropriate procedures are strictly followed and necessary documentation are in place. Ensure there is appropriate authorization.			
2	**Systems development**	Verify that there are defined criteria for adopting the use of a particular programming language or development tool for application development.	Insecure systems and unauthorized access.	Document standards and procedures for systems development.	
		Request for evidence of system requirement definition as well as analysis and design documentations from the System Analysts for system development and implementation.			

S/No.	Audit Entity	Test Procedures	Risk	Control	IS Security & Control Framework Reference
		Verify the programing language/environment being used and ensure that the tools are genuine and licensed software.			
		Verify that there is adequate access control in development environments to ensure security, which will prevent developers from using different versions of development environments to code applications.			
		Verify that the development environment is separated both physically and logically from the test and live environments.			
3	**Systems Testing**	Verify that the test and production environments are logically separated to enforce adequate security of data.	Unauthorized access.	Document access control procedures.	
		Verify that developers do not have access to production databases and as well as live applications.			
		Verify that applications are tested extensively and appropriate sign off are obtained from relevant stakeholders before deployment to live environment.	Failure of functionality and security.	Document a test procedure and ensure it is approved.	
4	**Change control**	Request for change management documentations for previous changes made on applications and ensure that necessary approvals were obtained in line with the organization change management policy and procedures.	Service disruptions due to Unauthorized changes	Document a test procedure and ensure it is approved.	
		Verify that application maintenance, patch deployment and upgrades are subjected to change management procedures.			
5	**Access control**	Verify that adequate access control mechanisms are implemented on the test and production environments with more security emphasis on live environment.	Unauthorized access and modification to live systems.	Separate production environment from test systems.	

S/No.	Audit Entity	Test Procedures	Risk	Control	IS Security & Control Framework Reference
		Verify that production data are not use as test data in the test environment and determine who has access to the test data.			
		Obtain the list of applications developed and maintained by BPR department. Review security and functional requirements of the applications based on documented system requirement. Review users access rights on the application as well as on the database and ensure that the security settings databases are adequate.	Unauthorized access and modification to live systems.	Implement adequate logical access control mechanism on the production environment to ensure accountability and non-repudiation of actions.	
		Review the security configurations of the web servers hosting the development, test and production environment of all applications developed by BPR unit including their operating systems security controls. Ensure that security configurations of production web servers are adequate to assure system security.		Ensure strong security configurations.	
		Verify that there is adequate separation of duties between developers, operators and administrators of the applications/web portals and their respective databases. Ensure that accountability and responsibilities for system functions are clearly defined and established.	Unauthorized access or privilege creeps due to lack of separation of duties.	Job segregation	
		Review data backup procedures for all applications/portals and their associated databases to ensure that data are backed up and securely retained.	Data loss	Secure backup for application data as well as source code.	
6	**Documentations**	Verify that there are adequate program documentations for all applications.	Inability to provide support to users and ensure job succession	Ensure that procedures for program	

S/No.	Audit Entity	Test Procedures	Risk	Control	IS Security & Control Framework Reference
			due to lack of program documentation.	documentation are approved and applied.	
		Verify that necessary approvals were obtained at all stages of application development process in conformity with established procedures and satisfaction of business and security requirements.			
		Verify the role of System Control personnel in the system development process and ensure that are the adequate documentation for all roles in the procedure manual?			
		Verify that the following documentation are in place for every in house developed application. 1. Project initiation document 2. System specification/design document 3. Process mapping/work flow diagram. 4. User manual 5. Technical manual/documentations 6. Lessons learnt. 7. Data Dictionary.			
7		Determine if BPR staff members have adequate training and competence required to deliver user requests for automation of processes.	Systems not meeting user requirements.	Provide adequate and required training.	
		Determine the adequacy of staffing in BPR unit.	Inability of the unit to deliver jobs on schedule due to lack of manpower.	Provide staff resource for all vacant positions.	
	Code Review & Vulnerability Assessment	Ensure that there is a procedure for the review of codes for newly developed applications as well as changes to existing applications.	Risk of non-detection of errors, malicious codes, wrong business logics, weak codes, which could	Code Review	

S/No.	Audit Entity	Test Procedures	Risk	Control	IS Security & Control Framework Reference
			result to control failure or financial loss.		
		Does the procedure for code review assign responsibilities for the exercise to specific department and person such that will ensure separation of duties (i.e. reviewer different from developer)?			ISO 27001 Clause A.6.1.2 Control Requirements: Conflicting duties and areas of responsibilities shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
		Verify that codes of newly developed applications and changes to the existing ones are reviewed for common errors, bugs, logical dysfunction, wrong business logics, etc, to ensure security and minimal impact on business.			ISO 27001 Clause A.14.2.3 Control Requirements: When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
		Verify that the outcome of the code review are reported as well as escalated for immediate actions and remediation. Request for evidence of review as well as escalation.			ISO 27001 Clause A.14.2.3 Control Requirements: When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

S/No.	Audit Entity	Test Procedures	Risk	Control	IS Security & Control Framework Reference
		Verify that technical vulnerabilities associated with software development have been identified, documented and the bank's exposure to them evaluated.	Risk of non-detection of common coding errors, poor coding standards, bugs, that create vulnerabilities, which could be exploited by hackers to compromise the applications, its data or the bank's system.	Perform vulnerability assessment and scan.	ISO 27001 Clause A.14.2.3 Control Requirements: Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
		Verify that vulnerability assessments/scans are being carried out on newly developed applications as well as changes made to existing applications.			ISO 27001 Clause A.14.2.3 Control Requirements: Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
		Are software tools acquired and being used to perform vulnerability scans (e.g Acunetix) and what is the frequency of this exercise for application already in production?			ISO 27001 Clause A.14.2.3 Control Requirements: Information about technical vulnerabilities of information systems being used shall be obtained in a timely

S/No.	Audit Entity	Test Procedures	Risk	Control	IS Security & Control Framework Reference
					fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
		Verify that the outcome of the vulnerability assessments/scans are reported as well as escalated for immediate actions and remediation. Request for evidence of scans as well as escalations.			ISO 27001 Clause A.14.2.3 Control Requirements: Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Prepared By: **Audit Team**