

Risk and Control Matrix

Table of Contents

- 1. IS GOVERNANCE2
- 2. SECURITY – LOGICAL AND PHYSICAL4
- 3. OPERATIONS.....6
- 4. EXTERNAL VENDORS, THIRD PARTY SERVICES.....8
- 5. BUSINESS CONTINUITY9
- 6. PROJECT MANAGEMENT AND SYSTEM DEVELOPMENT 10
- 7. APPLICATION MANAGEMENT 12

1. IS Governance

Objective:	To assess adequacy of management of IS within the organisation.	Impact: H/M/L		Impact explanation:				
High level controls:				Objective met by high level controls? (Yes/No)		Action ref:		
Threats	Flow-chart ref	Like-lihood H/M/L	Gross Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
1. Staff not aware of IS Strategy								
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
2. IS Strategy (local) does not align with business requirements and company direction.								
3. Quality of IS work is affected due to insufficient or inappropriate skilled resource in-house.								
4. Future hardware and software provisions are not planned and catered for.								
5. Ineffective communication between Regional IS and Hubs to clearly understand regional initiatives and global programme changes..								
6. IS activities and expenditure not managed, monitored and periodically and timely reported to regional and local mgt.								

7. IS expenditure not tracked against budget to clearly detail level of spending for each expenditure class.							
8. No policies or approved procedures to govern/ provide guidance over IS.							
9. Future business requirements for IT are not considered, planned and implemented in a timely fashion.							
10. Lack of integration between IS and business packages							

2. Security – Logical and Physical

Objective:	To ensure that all assets are properly safeguarded.	Impact: H/M/L		Impact explanation:				
High level controls:				Objective met by high level controls? (Yes/No)		Action ref:		
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
Logical								
1. Security management is reactive rather than proactive. No monitoring or auditing of user breaches is performed, reliance is primarily on user to inform.								
2. End –user password controls (including supervisors’) over access to the system and application are weak ie: a. No periodic force change b. Easy to guess c. No minimum length								
3. No precautions (procedures and software) are in place to prevent and detect the introduction of malicious software.								
Physical								
1. Access to work areas is not restricted to public.								
2. Stairwells and backdoors are not secured during business hours.								
3. Computer room is accessible to all staff								

3. Operations

Objective:	IS service is performed effectively and efficiently.	Impact: H/M/L		Impact explanation:				
High level controls:				Objective met by high level controls? (Yes/No)		Action ref:		
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
1. Agreed service levels are consistently not monitored, measured or met.								
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
2. No service levels (KPI) developed to establish benchmark for performance. 99.95% sys avail.								
3. Resource capacity focussing on mgt of infrastructure components are not monitored and measured, resource utilisation trends are not collected, analysed and reported on.				•				
4. No Help desk or similar service is provided to assist users with technical / IS related problems								
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
5. Determine that an individual has been assigned the responsibility for recording and tracking the								

software products installed onto information systems and PC's.							
6. Unauthorised software may be downloaded from the Internet or external sources. No processes in place to capture software loaded within the entity.							
7. Users are not aware of proper security procedures. Supporting documentation are not clearly defined and responsibilities over security not assigned.							
8. Determine how policies and standards are received and distributed to ensure appropriate staff is informed of changes to versions residing on site. Determine if a process exists to maintain local procedure documents if they exist.							

4. External vendors, third party services

Objective:	Services from third parties are formalised and managed to ensure that they are delivered according to requirements	Impact: H/M/L	H	Impact explanation:				
High level controls:				Objective met by high level controls? (Yes/No)		Action ref:		
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
1. No valid (signed) contracts with third parties.								
2. Services not monitored to determine compliance with agreed service levels.								
3. Lack of documentation from external vendor.								

5. Business continuity

Objective:	Assess that business and systems are suitable prepared to efficiently return to suitable operations in the event of a disaster.	Impact: H/M/L	H	Impact explanation:				
High level controls:				Objective met by high level controls? (Yes/No)		Action ref:		
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
1. No BCP has been developed or if one exists, is not up to date.								
2. Disaster recovery plan for IS is independent from overall BCP. No involvement from business unit managers in the documentation of BCP i.e. no formal sign off required								
3. DRP and BCP are not tested to ensure workability.								
4. Backups not suitably performed to adequately cover all systems and timings.								

6. Project Management and system development

Objective:	Structured, controlled processes are applied to managing projects and system development activities.	Impact: H/M/L	H	Impact explanation:				
High level controls:				Objective met by high level controls? (Yes/No)		Action ref:		
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
1. Systems are developed without reference to structured guidelines and best practices..								
2. No methodology/ structured procedures are applied to system development or project management.								
3. Determine whether priorities are assigned to the change requests and if so, how these are assigned. If priorities are assigned, assess controls to ensure changes processed in order.								
4. No process in place to control and monitor change requests (central repository and ageing mechanism). Outstanding requests are unresolved for long periods.								
5. Tested in not performed in a segregated/ controlled environment (a testing/QA region which is separate from development and production).								

6. Once migrated into the testing/quality assurance environment, code is not 'frozen' and susceptible to further change.							
7. Problems encountered during the testing and acceptance phase of the change methodology are not documented, followed-up and resolved. Test results are not reviewed and approved by the user through formal user acceptance process.							

7. Application Management

Objective:	To ensure that applications are suitably managed to allow	Impact: H/M/L		Impact explanation:				
High level controls:				Objective met by high level controls? (Yes/No)	No.	Action ref:		
Threats	Flow-chart ref	Like-lihood H/M/L	Risk H/M/L	Controls in place	Control strength H/M/L	Residual risk H/M/L	Action ref	
1. Reliant on bespoke applications that are not easily supported due to specialist skill required.								
2. Applications are not regularly updated or new revisions installed to maintain latest version and functionality.								
3. Applications are purchased and installed with no consideration for the business direction or compliance with the applications to support business strategy.								
4. Robust criteria is not applied during software procurement to indicate openness of process and clarity of consideration factors.								
5. Data extraction or reporting is weak and does not comply with Head Office requirements. Manual operations weekly to meet office requirements.								