Annex

Annex 1: Detailed Audit checklist from RISA Guidelines on IT Audit

N	CONTROL	AVAILABILITY (Yes/No)	RANKING (/10)	BRIEF COMMENTS
A	**ACCESS CONTROL POLICY AND PROCEDURES**			
A1	Do you have a clear Access Control Policy, approved by management, communicated to all users and reviewed regularly?			
A2	Are the clear procedures for account registration, modification and deregistration (including temporary account locking) in place?			
A3	Is each user allocated a unique password and user account?			
A4	Are individual roles and responsibilities considered when granting users access privileges?			
A5	Do you review user access privileges on a regular basis? (Including approval by supervisors)			
A6	Do you control password new/reset right, use secure channel to transmit new/reset passwords and ensure they are changed on first logon?			
A7	Do you enforce strong passwords and regular change of passwords?			
A8	Do you have tools or procedures in place to limit unsuccessful login attempts?			
A9	Do terminals/ sessions log off after a set period of time?			
A10	Is remote access closed by default, and any remote connection approved by the management?			
A11	Are logs generated and reviewed for all remote connections?			
A12	Are the wireless networks using strong authentication protocols and encryption?			
A13	Is the wireless network for guests connected to the corporate network?			
A14	Are devices identified when connected to corporate Wi-Fi/LAN?			
A15	Does the network require authentication to access it (LAN/Wi-Fi)			

A16	Does the institution perform risk assessment before allowing mobile devices on any system?			
A17	Is information classification implemented in the institution?			
B	**SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**			
B1	Does the institution have an information security awareness program and already running? Or is this a new concept for the institution?			
B2	Do you run any security training to all information system users in your institution?			
C	**AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**			
C1	Are auditable events clearly defined with audit frequency, and audit records?			
D	**SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES**			
D1	Do you have documented/shared Information security policy in place?			
D2	Is the institution conducting a periodic security assessment?			
D3	Are there reports and the results of that assessment? Are recommendations implemented?			
D4	Does your institution develop, update and document a critical infrastructure and its protection plan?			
E	**CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**			
E1	Does the institution develop, document and maintain baseline configuration of the information system? Do you have a change management procedure?			

E2	Does the institution define list of prohibited or restricted functions, ports, protocols and/ or services?			
F	**BUSINESS CONTINUITY PLANNING POLICY AND PROCEDURES**			
F1	Does the institution develop a business continuity plan and periodically tested to ensure continuity during disaster?			
F2	Is there any responsible person or team of Business continuity? Are they trained?			
F3	Does the institution have more than one (1) alternate service provider to support information system?			
F4	Does the institution conduct a periodic information backup to support the recovery time? Manual or automated?			
F5	Are all changed programs immediately backed up?			
G	**INCIDENT RESPONSE POLICY AND PROCEDURES**			
G1	Do you follow appropriate incident handling procedures?			
G2	Does this procedure define clear escalation process for incident handling			
G3	Is that procedure known by all staff and all incidents documented?			
H	**SYSTEM MAINTENANCE POLICY AND PROCEDURES**			
H1	Is there written standard for system maintenance? Are these standards reviewed regularly and approved?			
H2	Does maintenance support process ensure confidentiality of information			
H3	Are maintenance services provided by licensed/certified people/firm			
I	**MEDIA PROTECTION POLICY AND PROCEDURES**			

I1	Do you have a clear electronic media disposal Policy, approved by management?			
I2	Is there a secure store for electronics and physical media within a physically secure or controlled area (locked drawer, cabinet, or room, etc.)?			
I3	Is the area (in site/ off-site) access to electronic and physical media restricted only to authorized individuals? If yes, are media secured during transit to restricted area?			
I4	Does off- site Inventory/ storage regularly reviewed?			
J	**PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**			
J1	Is physical access restricted to selected employees?			
J2	Do you control all items brought into or taken out of the computer/server room?			
J3	Are sensitive application servers/ systems located in a physically restricted area?			
J4	Do you review physical access records/logs?			
J5	Do you test physical security controls on regular basis?			
K	**PERSONNEL SECURITY POLICY AND PROCEDURES**			
K1	Do your institution procedures address personnel screening and records of screened personnel (staff/third-party)?			
K2	Does your institution address personnel termination/transfer; records of personnel termination/transfer actions; list of information system accounts and relevant documents?			
L	**SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**			

L1	Has the institution integrated information security and information security risk management into their system development life cycle?			
L2	Does the institution include and consider security requirements in acquisition contracts?			
L3	Does the institution use software in accordance with contract agreements and copyright laws?			
L4	Does the institution enforce rules for user installed software on the information system and prohibited software?			
M	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**			
M1	Do you separate applications for users and managers/admin?			
M2	Do you have a mechanism to prevent unauthorised and unintended information transfer via shared system resources?			
M3	Do you have any information system that protects and prevents DoS?			
M4	Does the institution establish a continuous monitoring Strategy and reporting of the security status of the information system?			
M5	Do you have automated tools to support real-time analysis of events?			
N	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**			
N1	Do you have antivirus software and endpoint security installed in your systems? Do you automatically update them?			
N2	Has all staff been advised of the virus prevention procedures? (Awareness)			
N3	Do you centrally manage antivirus software and endpoint security?			
N4	Do you receive security alerts, advisories, and directives from designated external institutions?			

O	**DISASTER RECOVERY**			
O1	Does the contingency plan provide for recovery and extended processing of critical applications in the event of catastrophic disaster?			
O2	Are all recovery plans approved and regularly tested to ensure their adequacy in the event of disaster?			
O3	Are disaster recovery teams established to support disaster recovery plan?			
O4	Are responsibilities of individuals within disaster recovery team defined and time allocated for completion of their task?			
O5	Are priorities set for the recovery of critical systems?			
O6	Does the recovery plan ensure, in the event of failure: No loss of data received but not processed, no reprocessing of data already processed?			

Revision #5
Created 7 May 2025 09:43:36 by RISA
Updated 7 May 2025 11:18:02 by RISA