ISO 27001 BUSINESS CONTINUITY CHECKLIST

CYBERSHIELD

WHERE AWARENESS UNLOCK SECURITY

REQUIREMENT SECTION/ CATEGORY	ASSESSMENT	IN COMPLIANCE?	REMARKS
5. Information Security Policies			
5.1	Security policies exist?		
5.2	All policies approved by management?		
5.3	Evidence of compliance?		
6. Organization of information security			
6.1	Defined roles and responsibilities?		
6.2	Defined segregation of duties?		
6.3	Verification body / authority contacted for compliance verification?		
6.4	Established contact with special interest groups regarding compliance?		
6.5	Evidence of information security in project management?		
6.6	Defined policy for working remotely?		
7. Human resources security			

7.1	Defined policy for screening employees prior to employment?		
7.2	Defined policy for HR terms and conditions of employment?		
7.3	Defined policy for management responsibilities?		
7.4	Defined policy for information security awareness, education, and training?		
7.5	Defined policy for disciplinary process regarding information security?		
7.6	Defined policy for HR termination or change-of-employment policy regarding information security?		
8. Asset management			
8.1	Complete inventory list of assets?		
8.2	Complete ownership list of assets?		
8.3	Defined "acceptable use" of assets policy?		
8.4	Defined return of assets policy?		
8.5	Defined policy for classification of information?		
8.6	Defined policy for labeling information?		
8.7	Defined policy for handling of assets?		
8.8	Defined policy for management of removable media?		
8.9	Defined policy for disposal of media?		
8.10	Defined policy for physical media transfer?		
9. Access control			
9.1	Defined policy for access control policy?		

9.2	Defined policy for access to networks and network services?		
9.3	Defined policy for user asset registration and de-registration?		
9.4	Defined policy for user access provisioning?		
9.5	Defined policy for management of privileged access rights?		
9.6	Defined policy for management of secret authentication information of users?		
9.7	Defined policy for review of user access rights?		
9.8	Defined policy for removal or adjustment of access rights?		
9.9	Defined policy for use of secret authentication information?		
9.10	Defined policy for information access restrictions?		
9.11	Defined policy for secure log-in procedures?		
9.12	Defined policy for password management systems?		
9.13	Defined policy for use of privileged utility programs?		
9.14	Defined policy for access control of program source code?		
10. Cryptography			
10.1	Defined policy for use of cryptographic controls?		
10.2	Defined policy for key management?		
11. Physical and environmental security			
11.1	Defined policy for physical security perimeter?		
11.2	Defined policy for physical entry controls?		

11.3	Defined policy for securing offices, rooms, and facilities?		
11.4	Defined policy for protection against external and environmental threats?		
11.5	Defined policy for working in secure areas?		
11.6	Defined policy for delivery and loading areas?		
11.7	Defined policy for equipment siting and protection?		
11.8	Defined policy for supporting utilities?		
11.9	Defined policy for cabling security?		
11.10	Defined policy for equipment maintenance?		
11.11	Defined policy for removal of assets?		
11.12	Defined policy for security of equipment and assets off premises?		
11.13	Secure disposal or re-use of equipment?		
11.14	Defined policy for unattended user equipment?		
11.15	Defined policy for clear desk and clear screen policy?		
12. Operations security			
12.1	Defined policy for documented operating procedures?		
12.2	Defined policy for change management?		
12.3	Defined policy for capacity management?		
12.4	Defined policy for separation of development, testing, and operational environments?		
12.5	Defined policy for controls against malware?		

12.6	Defined policy for backing up systems?		
12.7	Defined policy for information backup?		
12.8	Defined policy for event logging?		
12.9	Defined policy for protection of log information?		
12.10	Defined policy for administrator and operator log?		
12.11	Defined policy for clock synchronization?		
12.12	Defined policy for installation of software on operational systems?		
12.13	Defined policy for management of technical vulnerabilities?		
12.14	Defined policy for restriction on software installation?		
12.15	Defined policy for information system audit control?		
13. Communication security			
13.1	Defined policy for network controls?		
13.2	Defined policy for security of network services?		
13.3	Defined policy for segregation in networks?		
13.4	Defined policy for information transfer policies and procedures?		
13.5	Defined policy for agreements on information transfer?		
13.6	Defined policy for electronic messaging?		
13.7	Defined policy for confidentiality or non-disclosure agreements?		
13.8	Defined policy for system acquisition, development, and maintenance?		

14. System acquisition, development, and maintenance			
14.1	Defined policy for information security requirements analysis and specification?		
14.2	Defined policy for securing application services on public networks?		
14.3	Defined policy for protecting application service transactions?		
14.4	Defined policy for in-house development?		
15. Supplier relationships			
15.1	Defined policy for supplier relationships?		
16. Information security incident management			
16.1	Defined policy for information security management?		
17. Information security aspects of business continuity management			
17.1	Defined policy for information security continuity?		
17.2	Defined policy for redundancies?		
18. Compliance			
18.1	Defined policy for identification of applicable legislation and contractual requirement?		
18.2	Defined policy for intellectual property rights?		
18.3	Defined policy for protection of records?		
18.4	Defined policy for privacy and protection of personally identifiable information?		
18.5	Defined policy for regulation of cryptographic control?		
18.6	Defined policy for compliance with security policies and standards?		
18.7	Defined policy for technical compliance review?		

Checked by ________________________________

Date ____________________________________

DISCLAIMER

Any articles, templates, or information provided by CyberShield Tanzania inc. on the website are for reference only. While we strive to keep the information up to date, relevance and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk and we shall not guarantee claim.

This template is provided as a sample only. This template is in no way meant as legal or compliance advice. Users of the template must determine what information is necessary and needed to accomplish their objectives. Your advice to visit the institutional website to understand how to use the checklist, in regard to brief information that we provide here.