CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Policies for information security*	**Is there a comprehensive, documented information security policy?**	
Control Statement	*Information security roles and responsibilities*	**Have roles and responsibilities been defined for all functions and individuals who are part of the security workforce?**	
Control Statement	*Management responsibilites*	**Is ownership of critical information and systems clearly defined and assigned to named indivintuals who have accepted their responsibilities?**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Information security in project management*	**Are projects(and security-related initiatives) run in a structured, systematic and consistent manner, in line with the organizations standard project management process?**	
Control Statement	*Inventory of information and other associated assets*	**Are important details about all types of assets recorded in registers or equivalent?**	
Control Statement	*Return of assets*	**Are applicants for employment subjected to a comprehensice screening process prior to commencing work?**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Calssification of information*	**Is critical and sensitive information(in digital, physical or cognitive form) protected at each stage of the information lifecycle(create, process, transmit, store and delete)?**	
Control Statement	*Access control*	**Is there an access control policy that defines security requirments, including the need for least privilege, individual accountability and privilege access management?**	
Control Statement	*Identity management*	**Is access to systems, applications,networks,collaboration platforms and endpoint devices restricted by access control mechanisms, such as passwords/passphrases, tokens or biometrics**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Access rights*	**Is there an approved process for providing entities(typically users and sometimes services) with appropriate accounts(e.g. User IDs),access privileges(or rights), and permissions?**	
Control Statement	*Monitoring , review and changemanagement of supplier services*	**The organization should regularly monitor, review , evaluate and manage change in supplier information security practices and service delivery?**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Information security incident management planning and preparation*	**Has a framework beenestablished for managing information security incidents, which covers the people, processes and technology required to handle incidents quickly and effectively?**	
Control Statement	*Assessment and decision on information security events*	**Has a comprehensive security event management process beenestablished to identify, investigate and help respond to security related events?**	
Control Clause	***People Controls***	***Question***	
Control Statement	*Screening*	**Are applicants for employment subjected to a comprehensice screening process prior to commencing work?**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Terms and conditions of employment*	**Do key employment-relateddocuments(e.g. job descriptions or terms and conditions of employment) clearly specify the information security responsibilities of individuals?**	
Control Statement	*Information security awareness, education and training*	**Are specific security, education, training and awareness activities undertaken, including the creation of awareness training programme, to promote and embed expectedsecurity behaviour?**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Remote working*	**Are employee-owned devices(e.g. smartphones, tablets and laptops),used for business purposes, permitted only if they meet an agreed specification and have been autorised for use?**	
Control Clause	***Physical Controls***	***Question***	
Control Statement	*Physical security controls*	**Have information security requirments been documented for each stage of the physical premises lifecycle ?**	
Control Statement	*Physical entry controls*	**Have physical risk assessments been performed for new and existing locations, particularly critical facilities?**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Securing office, rooms and facilities*	**Have information security requirments been documented for each stage of the physical premises lifecycle ?**	
Control Statement	*Physical security monitoring*	**have intruder detection systems been installed and periodically tested to protect critical facilities?**	
Control Statement	*Protecting against physical and enviromental threats*	**Is the availability of power supplies to critical facilities assured (e.g. by providing uninterruptable power supply(UPS) devices and backup electricity generators that are maintained and tested regularly)?**	
Control Clause	***Technological Controls***	***Question***	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Privileged access rights*	**Is there an approved process for providing entities(typically users and sometimes services) with appropriate accounts(e.g. User IDs),access privileges(or rights), and permissions?**	
Control Statement	*Information access restriction*	**Is access to systems, applications,networks,collaboration platforms and endpoint devices restricted to authorised individuals?**	
Control Statement	*Secure Authentication*	**Is access to systems, applications, networks, collaboration platforms and endpoint devices restricted by access control mechanisms, such as passwords/passphrases, tokens or biometrics?**	

CyberVitals Checklist			
Control Clause	***Organizational Controls***	***Question***	***Y/N***
Control Statement	*Protection against malware*	**Are users made aware of the actions required to minimize the risks associated with malware?**	
Control Statement	*Information Backup*	**Are backups of essential information and software performed frequently enough to meet business and security requirements?**	
Control Statement	*Web filtering*	**Is website content(e.g. configuration files, web pages and images) protected against corruption and unauthorised disclosure?**	
Control Statement	*Use of cryptography*	**Has a process been established for managing compliance with relevant legal and regulatory requirments affecting information security across the organisation?**	