ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
ISO27001	**5**	**Organisational Controls**										
ISO27001	5.1	Policies for Information Security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur	To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business requirements, legal, statutory, regulatory and contractual requirements.	Identify	Governance	Access Governance	Group information security policy and related policy documents provides guidance for ISMS implementation. It ensures management direction and support for information security in accordance with business requirements and relevant laws and regulations aligned to business objectives.	Yes	Yes	Yes	Yes
ISO27001	5.2	Information Security Roles and Responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.	Identify	Governance	Access Governance	Clear definition and designation of information security roles and responsibilities, authorities and the hierarchy enables management of ISMS and provides ownership.	Yes	Yes	Yes	Yes
ISO27001	5.3	Segregation of Duties	Conflicting duties and areas of responsibility should be segregated.	To reduce the risk of fraud, error and bypassing of information security controls.	Protect	Governance	Access Governance	BCX Host the Infrastructure. Roles and Responsibilities within BCX should be defined for managing the Infrastructure. In SOW Customers define roles and responsibilities, and allocates rights for service providers. Scope of ISMS is restricted to support phase of service fulfilment life cycle.	Yes	Yes	Yes	Yes
ISO27001	5.4	Management Responsibilities	Management should be a role model for information security and require all	To ensure management understand their role in information security and undertake actions	Identify	Governance	Access Governance	It is organisational practices for management to take ownership and responsibilities to ensure employees	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization	aiming to ensure all personnel are aware of and fulfil their information security responsibilities				comply with corporate policies. This is to ensure employee protect information while carrying out the responsibilities.				
ISO27001	5.5	Contact with Authorities	The organization should establish and maintain contact with relevant authorities.	To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities		Governance	Security Incident Management	BCX Host the Infrastructure. Appropriate contacts with relevant authorities should be maintained. Correct and up to date Contact information is required for notification of Security violations and Security Incidents. POPI Regulations.	Yes	Yes	Yes	Yes
ISO27001	5.6	Contact with Special Interest Groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations	To ensure appropriate flow of information takes place with respect to information security.		Governance	Security Incident Management	BCX forms part of several special interest groups such as Microsoft, Citrix and Information Security Forum. Updates are shared regarding security vulnerabilities or upgrades to systems through these forums.	Yes	Yes	Yes	Yes
ISO27001	5.7	Threat Intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence	To provide awareness of the threat environment that can impact the organization so that the organization can take appropriate mitigation actions		Threat and Vulnerability Management	Vulnerability Exposure	BCX aims to provide secure platforms to internal users and customers. In order to understand the threats related to customers it is imperative that threat intelligence be collected, analysed and actioned where appropriate.	Yes	In planning	Yes	In planning
ISO27001	5.8	Information Security in Project Management	Information security should be integrated into the organization's project	To ensure information security risks related to projects and deliverables are efficiently and effectively		Governance	Data Protection	Information Security should be Considered in any Lifecycle of Project management to ensure information security	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			management activities	included in project management activities throughout the project lifecycle				requirements are designed and built into business solutions/services. Confidential information should not be shared with Non-Interested Parties at any stage of a Projects Life Cycle. This is specific for enhancements to existing information systems. This is an ongoing action based on Hotnews and critical vulnerabilities identified by different sources.				
ISO27001	5.9	Inventory of Information and Other Associated Assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership		Asset Management	Data Protection	It is required that managed customer's assets and service support information are recorded and maintained to provide accurate support and protection as per regulations. To ensure accountability and that responsibilities are carried out, ownership for capturing and maintenance of assets must be allocated.	Yes	Yes	Yes	Yes
ISO27001	5.10	Acceptable Use of Information and other Associated Assets	Rules for the acceptable use and procedures for the handling of information and other associated assets should be identified, documented and implemented.	To ensure information and other associated assets are appropriately protected, used and handled		Information Protection	Data Protection	This is required to ensure customer information is managed as per requirements, regulatory and laws. Handling procedures are required to ensure personnel handle information in secured manner during processing, storage, transmission and destruction. -	Yes	Yes	Not Applicable	No

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
								Infrastructure Decommissioning Process should include the Sanitisation to ensure no Asset that is removed from the Infrastructure contains any Customer, System or Asset Information				
ISO27001	5.11	Return of Assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement	To protect the organization's assets as part of the process of changing or terminating employment or contract.		Asset Management	Data Protection	It is an organisational requirement that all assets are returned upon termination of employment, this will minimise the risk of data theft and unauthorised access. Return of assets after termination are managed through HR process. ITS procurement manages the collection and reallocation of assets. Reuse of mobile devices are formatted before reallocation as part of ITS asset management.	Yes	Yes	Not Applicable	No
ISO27001	5.12	Classification of Information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements	To ensure identification and understanding of protection needs of information in accordance with its importance to the organization		Information Protection	Data Protection	Classifying assets helps in implementing controls required that information assets receive the desired level of protection. It is organisational policy that assets are classified as per classification policy.	Yes	Yes	Not Applicable	No
ISO27001	5.13	Labelling of Information	An appropriate set of procedures for information labelling should be developed and	To facilitate the communication of classification of information and support automation of information		Information Protection	Data Protection	Labelling of assets helps in providing guidance on how information must be handled when processed and stored, this must be	Yes	Yes	Not Applicable	No

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			implemented in accordance with the information classification scheme adopted by the organization	processing and management				done as per organisational policy.				
ISO27001	5.14	Information Transfer	Information transfer rules, procedures, or agreements, both within the organization and between the organization and other parties, should be in place for all types of transfer facilities	To maintain the security of information transferred within an organization and with any external interested party		Information Protection	Data Protection	The organisational policy provides direction for the implementation of procedures required to comply with legal, regulatory and contractual requirements. This control is required to ensure agreements with external providers include clause for secure transfer of information. Example Veritas Netbackup Appliance Layered Security which includes Security controls.	Yes	Yes	Not Applicable	No
ISO27001	5.15	Access Control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements	To ensure authorized access and to prevent unauthorized access to information and other associated assets		Identity and Access Management	Access Governance	This ensures that access to BCX and customer's information and information processing systems is provided based on the role addressing the information security requirements as per organisational policy.	Yes	Yes	Yes	Yes
ISO27001	5.16	Identity Management	The full lifecycle of identities should be managed	To allow for the unique identification of individuals and systems accessing the organisation's information and other associated assets, and to enable appropriate		Identity and Access Management	Access Governance	Users must be registered after due approvals and de-registered in case of resignation or change in departments to prevent unauthorised access.	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
				assignment of access rights								
ISO27001	5.17	Authentication Information	Allocation and management of authentication information should be controlled by a management process, including advising personnel of appropriate handling of authentication information	To ensure proper entity authentication and prevent failures of authentication processes		Identity and Access Management	Access Governance	Access Control Policy and Procedures should be adhered to, to ensure no Unauthorised Access to systems including Laptops. Access to application information is Controlled by the Customer. This control Should be managed at organisational level and customer environment are enforced through partner Cloud Design requirements. This control is required to ensure support privileged credentials are handled and protected to prevent unauthorized access to the systems and data.	Yes	Yes	Yes	Yes
ISO27001	5.18	Access Rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy and rules on access control.	To ensure only authorized access to information and other associated assets		Identity and Access Management	Access Governance	This control is adopted to ensure access is provisioned in accordance with organisational access control policy and minimise unauthorised access. Regular review of user access rights is required to ensure that no user gets elevated access as a result of accumulation of rights or change of role and minimise unauthorised access. Removal of user access rights is	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
								required to ensure that no user gets elevated access as a result of accumulation of rights or change of role and minimise unauthorised access.				
ISO27001	5.19	Information Security in Supplier Relationships	Processes and procedures should be identified and implemented to manage the information security risks associated with the use of supplier's products or services	To maintain an agreed level of information security in supplier relationships		Supplier Relationships Security	3rd Party Security	Information Security should include Supplier Code of Conduct and NDA. Information security needs to be addressed as per the access to information per supplier.	Yes	Yes	Yes	Yes
ISO27001	5.20	Addressing Information Security within Supplier Agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship	To ensure information security of the organization in supplier relationships		Supplier Relationships Security	3rd Party Security	Information Security should include Supplier Code of Conduct and NDA, MSA and/or Statement of Work	Yes	Yes	Yes	Yes
ISO27001	5.21	Managing Information Security in the ICT Supply Chain	Processes and procedures should be defined and implemented to address information security risks associated with ICT services and product supply chain	To ensure information security of the organization in ICT supply chain		Supplier Relationships Security	3rd Party Security	Information Security should be addressed throughout the ICT supply chain process.	Yes	Yes	Yes	Yes
ISO27001	5.22	Monitoring, Review and Change Management of Supplier Services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	To maintain an agreed level of information security and service delivery in line with supplier agreements		Supplier Relationships Security	3rd Party Security	MSA and Underpinning Contracts should be formalised to Monitor and manage Services from Suppliers if required. Supplier performance should be reviewed in line	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
								with deliverables/SLAs.				
ISO27001	5.23	Information Security for Use of Cloud Services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements	To specify and manage information security for the use of cloud services.		Supplier Relationships Security	3rd Party Security	To ensure that BCX and customer information is protected for information security in the cloud environment. Cloud exclusion - Cloud platforms do not make use of additional cloud services.	Yes		Not Applicable	No
ISO27001	5.24	Information Security Incident Management Planning and Preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities	To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.		Information Security Event Management	Security Incident Management	Security Incident Management Procedures should be included in the Organisation Incident Management Process	Yes	Yes	Yes	Yes
ISO27001	5.25	Assessment and Decision on Information Security Events	The organization should assess information security events and decide if they are to be categorized as information security incidents	To ensure effective categorization and prioritization of information security events.		Information Security Event Management	Security Incident Management	Information security events must be prioritised based on selected classification. The Organisation must determine the correctness of the classification and adjust accordingly.	Yes		Yes	Yes
ISO27001	5.26	Response to Information Security Incidents	Information security incidents should be responded to in accordance with the documented procedures	To ensure efficient and effective response to information security incidents		Information Security Event Management	Security Incident Management	Security Incident Management Procedures should be included in the Organisation Incident Management Process	Yes	Yes	Yes	Yes
ISO27001	5.27	Learning from Information Security Incidents	Knowledge gained from information security incidents should be used to strengthen and	To reduce the likelihood or impact of future incidents		Information Security Event Management	Security Incident Management	This control is required to ensure root cause analysis actions are initiated for information security incidents to	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			improve the control environment					ensure lessons are learned.				
ISO27001	5.28	Collection of Evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of information from information security incidents.	To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal action.		Information Security Event Management	Security Incident Management	This control is required to ensure collected information security incidents information can be admissible in court and done as per organisational policy.	Yes	Yes	Yes	Yes
ISO27001	5.29	Information Security During Disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	To provide information and other associated asset with adequate protection during disruption		Continuity	Security Incident Management	Business continuity is critical for BCX. This control is adopted to ensure information security (CIA) is made part of BCP process. This control ensures that BCP consider information security requirements. This control is adopted to test the effectiveness and efficiency of the BCP/DRP of BCX in accordance of the above two controls.	Yes	Yes	Yes	Yes
ISO27001	5.30	ICT Readiness for Business Continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements	To ensure the availability of the organization's information and other associated assets in the event of a disruption.		Continuity	Security Incident Management	Business continuity is critical for BCX. This control is adopted to ensure information security (CIA) is made part of BCP process. This control ensures that BCP consider information security requirements. This control is adopted to test the effectiveness	Yes	Yes	Yes	Yes
ISO27001	5.31	Identification of Legal, Statutory, Regulatory and Contractual Requirements	Information security relevant legal, statutory, regulatory and contractual requirements and the organization's approach to	To ensure compliance with legal, statutory, regulatory or contractual requirements related to information security		Legal and Compliance	Security Compliance Management	BCX require it to adhere to contractual obligations, regulatory and legal requirements. This control is adopted to ensure that operations complies	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			meet these requirements should be identified, documented and kept up to date					with all applicable legislations, contractual obligations and in accordance with organisational policy. It is required to ensure any external/internal communication to and from the Cloud environment is subject to encryption controls across the boundaries to comply with relevant regulations, legislation and agreements. Cryptographic Controls should be in place where required when Asset Information is stored, processed and transported on Personnel Computers, USB devices or External devices.				
ISO27001	5.32	Intellectual Property Rights	Organizations should implement appropriate procedures should be implemented to protect intellectual property rights	To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products		Legal and Compliance	Security Compliance Management	BCX Only Host the Cloud Infrastructure. Customers application licenses are managed by the customer. Use of software copyright are defined within the Acceptable Use Policy End User devices are monitoring and use of unauthorised software are uninstalled as per software management policy requirements	Not Applicable		Not Applicable	
ISO27001	5.33	Protection of Records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized	To ensure compliance with legal, statutory, regulatory or contractual requirements related to the		Information Protection	Data Protection	This control is required to ensure records relating to support activities are protected in accordance with organisational policy.	Yes	Yes	Not Applicable	No

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			release, in accordance with legal, statutory, regulatory, contractual and business requirements	protection of records.								
ISO27001	5.34	Privacy and Protection of PII	The organization should identify and meet the requirements regarding preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	To ensure compliance with legal, statutory, regulatory or contractual requirements related to the information security aspects of the protection of PII.		Information Protection	Data Protection	This control is required to ensure privacy protection of personally identifiable information as per legal and regulatory requirements, and organisational policy.	Yes	Yes	Not Applicable	No
ISO27001	5.35	Independent Review of Information Security	The organization's approach to managing information security and its implementation including people process and technology should be reviewed independently at planned intervals, or when significant changes occur.	To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security		Information Security Assurance	Security Compliance Management	Management should initiate the independent review to ensure the continuing suitability, adequacy and effectiveness of the approach to managing information security.	Yes	Yes	Yes	Yes
ISO27001	5.36	Compliance with Policies and Standards for Information Security	Compliance with the organization's information security policy, topic-specific policies and standards should be regularly reviewed.	To ensure that information security is implemented and operated in accordance with the organizational policies topic-specific policies and standards.		Legal and Compliance	Security Compliance Management	This control is adopted so that the managers shall be able to identify how to review information security requirements defined in policies, standards and other applicable regulations are met. This control is selected to ensure technical compliance are reviewed to assess the level of compliance with policies, standards and other applicable	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
								regulations and are performed.				
ISO27001	5.37	Documented Operating Procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them	To ensure the correct and secure operation of information processing facilities		Continuity	Security Compliance Management	This control is required to ensure protection and retention of support documentation and knowledge transfer	Yes	Yes	Yes	Yes
ISO27001	**6**	**People Controls**										
ISO27001	6.1	Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis in accordance with applicable laws, regulations and ethics, and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment		Human Resource Security	Vulnerability Exposure	Background verification checks on candidates for employment is required accordance with laws, regulations of the organization and ethics proportional to the business and partners requirements. This is to minimize the risk of fraud and theft, as BCX processes customer sensitive data. Screening form part of the BCX HR recruitment process.	Yes	Yes	Yes	Yes
ISO27001	6.2	Terms and Conditions of Employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	To ensure personnel understand their information security responsibilities for the roles for which they are considered		Human Resource Security	Vulnerability Exposure	Contractual and confidentiality agreements are required at all organisational levels to protect company and customer information and interests.	Yes	Yes	Yes	Yes
ISO27001	6.3	Information Security Awareness, Education and Training	Personnel of the organization and relevant interested parties should receive appropriate information security	To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.		Human Resource Security	Security Training and Awareness	It is BCX organisational practices to follow a Security awareness program. This is to ensure employees are aware of their responsibilities and are educated of	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			awareness, education and training and regular updates of organizational policies and procedures, as relevant for their job function					information security threats.				
ISO27001	6.4	Disciplinary Process	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	To ensure personnel and other relevant interested parties understand the consequences of information security breaches, and non-compliant activities are deterred		Human Resource Security	Vulnerability Exposure	Disciplinary is organisational policy regarding any misconduct. Information security policies violations are handled through the process and must be included in all related polices. This is to enforce disciplinary behaviour among staffs and to make them aware of the fact that policies and processes exist and need to be complied with.	Yes	Yes	Yes	Yes
ISO27001	6.5	Responsibilities After Termination or Change of Employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	To protect the organization's interests as part of the process of changing or terminating employment or contract		Human Resource Security	Access Governance	It is BCX organisational practise to ensure revocation of employee's access when employee terminate employment or change of role. This is to minimise the risk of unauthorised or unintended access to information.	Yes		Yes	Yes
ISO27001	6.6	Confidentiality or Non-Disclosure Agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly	To maintain confidentiality of information accessible by personnel or external parties.		Human Resource Security	Vulnerability Exposure	Non Disclosure Agreements must be signed by all External Parties. **This is required to protect the Information of the Customer and IPR**	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			reviewed and signed by personnel and other relevant interested parties									
ISO27001	6.7	Remote Working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises	To ensure the security of information when personnel are working remotely.		System and Network Security	Data Protection	BCX recognises that more flexibility for employees, regarding their workplace and work hours, can improve employee engagement, performance, productivity and work life balance. The organisation is committed to supporting flexible and secure working arrangements.	Yes	Yes	Not Applicable	
ISO27001	6.8	Information Security Event Reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner	To support timely, consistent and effective reporting of information security events that can be identified by personnel		Information Security Event Management	Security Incident Management	Security Event Management should be included in the Organisation Event Management Process This control is required to ensure information security incidents are reported in accordance with legal and regulatory requirements, and meet organisational policy.	Yes	Yes	Yes	Yes
ISO27001	**7**	**Physical Controls**										
ISO27001	7.1	Physical Security Perimeter	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and other associated assets.	To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.		Physical Security	Data Protection	Physical Servers and Storage Devices are Hosted at the BCX Data Centres and these assets should be protected through secure zoning of areas data is stored and processed.	Yes	Yes	Yes	
ISO27001	7.2	Physical Entry Controls	Secure areas should be protected by appropriate entry	To ensure only authorized physical access to the		Physical Security	Data Protection	Physical Servers and Storage Devices are Hosted at the BCX Data Centres	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			controls and access points	organization's information and other associated assets occurs.				and these assets should be protected No delivery or Loading of support equipment with any Information Assets. Access point for Delivery or Loading of any equipment should however be controlled to prevent access to Premises that Hosts Information Assets				
ISO27001	7.3	Securing Offices, Rooms and Facilities	Physical security for offices, rooms, and facilities should be designed and implemented.	To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities		Physical Security	Data Protection	Physical Servers and Storage Devices are Hosted at the BCX Data Centres and these assets should be protected. This control is also required to ensure protection of employees and ensure compliance with legal and regulatory.	Yes	Yes	Yes	Yes
ISO27001	7.4	Physical Security Monitoring	Premises should be continuously monitored for unauthorized physical access	To detect and deter unauthorized physical access		Physical Security	Data Protection		Yes		Yes	Yes
ISO27001	7.5	Protecting Against Physical and Environmental Threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented	To prevent or reduce the impacts of events originating from physical and environmental threats		Physical Security	Data Protection	This control is required to ensure protection of employees and ensure compliance with legal and regulatory requirements.	Yes	Yes	Yes	Yes
ISO27001	7.6	Working in Secure Areas	Procedures for working in secure areas should be designed and implemented	To prevent damage and interference to the organization's information and other associated assets in secure areas		Physical Security	Data Protection	Access to secure offices must be restricted	Yes	Yes	Yes	Yes
ISO27001	7.7	Clear Desk and Clear Screen	Clear desk rules for papers and	To reduce the risks of		Physical Security	Data Protection	This control is required to ensure	Yes	Yes	Not Applicable	

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			removable storage media and clear screen rules for information processing facilities should be defined and enforced	unauthorized access, loss of and damage to information on the desks, screens and in other accessible locations during and outside normal working hours				protection of unattended workstations and classified printed information as per organisational policy from unauthorised access.				
ISO27001	7.8	Equipment Siting and Protection	Equipment should be sited securely and protected.	To reduce the risks from environmental threats and hazards, and opportunities for unauthorized access		Physical Security	Data Protection	Physical Servers and Storage Devices are Hosted at the BCX Data Centres and these assets should be protected FS - All assets must be secured	Yes	Yes	Yes	Yes
ISO27001	7.9	Security of Assets off-premises	Off-site assets should be protected taking into account the different risks	To prevent loss, damage, theft or compromise of off-site assets and interruption to the organization's operations		Asset Management	Data Protection	No Asset information should be moved off site. Assets such as Laptops that may contain Information Assets and move Off Site should be controlled FS - with WFH policy all assets are off site permanently. Validation via email	Yes	Yes	Not Applicable	
ISO27001	7.10	Storage Media	Storage media should be managed through its lifecycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	To ensure only authorized disclosure, modification, removal or destruction of information stored on media		Asset Management	Data Protection	Removable devices must be protected and secured from unauthorised access. This is adopted to ensure that media store data securely. It is organisational policy to encrypt storage devices. Equipment should be disposed through an approved Process. Disposal of Asset should be managed by a central department and proof of Disposal and sanitisation should be kept for record purposes Physical Media does not get Transferred	Yes	Yes	Not Applicable	

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
								but Media such as USB Devices, External Drives or even Laptops Containing Asset Information could be transferred and should be encrypted to protect data.				
ISO27001	7.11	Supporting Utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities	To prevent loss, damage or compromise of information and other associated assets due to the failure and disruption of supporting utilities or interruption to the organization's operations		Physical Security	Data Protection	Physical Servers and Storage Devices are Hosted at the BCX Data Centres and these assets should be protected from power failures and other disruptions caused by failures in supporting utilities	Yes	Yes	Yes	Yes
ISO27001	7.12	Cabling Security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage	To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations due to failure in power and communications cabling.		Physical Security	Data Protection	BCX is responsible for Lan networks and not the Wide area Network. BCX area of Responsibility of the Infrastructure should be protected for Interception, Interference or damaging of this infrastructure.	Yes	Yes	Yes	Yes
ISO27001	7.13	Equipment Maintenance	Equipment should be maintained correctly	To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations		Asset Management	Data Protection	Physical Servers are used as Hosting VMWARE. These Service should be on Maintenance Contract and Maintained according to the Maintenance plans FS - Servers are maintained inline with business requirement. Backup hardware is in place.	Yes	Yes	Yes	Yes
ISO27001	7.14	Secure Disposal or Re-use of Equipment	Items of equipment containing storage media should be verified to ensure that any	To prevent leakage of information from equipment to be disposed or re-used		Asset Management	Data Protection	Any Equipment/Storage that is Decommissioned should follow a Secure Decommissioning	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use					and Sanitisation Process				
ISO27001	**8**	**Technological Controls**										
ISO27001	8.1	User Endpoint Devices	Information stored on, processed by or accessible via user endpoint devices should be protected	To protect information against the risks introduced by using user endpoint devices		Information Protection	Data Protection	BCX Personnel and External consultants are allowed to utilise their own devices(This Include the use of Cell Phones) to support customers and this requires control and protection. Any Physical Equipment containing Information Asset should be controlled in a manner that no unauthorised access can be gained to these.	Yes	Yes	Not Applicable	No
ISO27001	8.2	Privileged Access Rights	The allocation and use of privileged access rights should be restricted and managed	To ensure only authorized users, software components and services are provided with privileged access rights.		Identity and Access Management	Access Governance	Support personnel are provided privileged access to customer's environment for provide support, this requires strict security management and monitoring.	Yes	Yes	Yes	Yes
ISO27001	8.3	Information Access Restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control	To ensure only authorized access and to prevent unauthorized access to information and other associated assets		Identity and Access Management	Access Governance	This control Should be managed at organisational level and customer environment are enforced through partner Cloud Design requirements.	Yes	Yes	Yes	Yes
ISO27001	8.4	Access to Source Code	Read and write access to source code, development tools and software libraries should be	To prevent the introduction of unauthorized functionality, avoid unintentional or malicious		Identity and Access Management	Access Governance	No Development is done within the Cloud Infrastructure environment and no Access to any Source Code.	na	No	Not Applicable	No

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			appropriately managed.	changes and to maintain the confidentiality of valuable intellectual property								
ISO27001	8.5	Secure Authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control	To ensure a user or an entity is securely authenticated when access to systems, applications, and services is granted		Identity and Access Management	Access Governance	Secure log-on is managed at organisational level and policy for log-on procedure controlled through IT policies. All applications are configured to use sign-on to ensure only authorised users access the information. Customer log-on are enforced through partner Cloud Design requirements.	Yes	Yes	Yes	Yes
ISO27001	8.6	Capacity Management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	To ensure the required capacity of information processing facilities		Continuity	Data Protection	Continuous Capacity Management is required to plan New Services and the Growth of Current Services.	Yes	Yes	Yes	Yes
ISO27001	8.7	Control Against Malware	Protection against malware should be implemented, supported by appropriate user awareness	To ensure information and other associated assets are protected against malware		System and Network Security	Malware Protection	End User Device's are not managed by BCX. For Customers but Internal Equipment are managed by Internal IT. Servers should be protected against Malware and Managed by BCX Server Support	Yes	Yes	Yes	Yes
ISO27001	8.8	Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate	To prevent exploitation of technical vulnerabilities		Threat and Vulnerability Management	Vulnerability Exposure	This control was selected to minimise risk of known OS and database vulnerabilities. Infrastructure vulnerability management is managed by BCX. This is specific for enhancements to existing information systems. This is an ongoing action	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			measures should be taken.					based on hot news. The COVID pandemic has in this time and place put a lot of focus on cybersecurity. This control is selected to ensure technical compliance are reviewed to assess the level of compliance with policies, standards and other applicable regulations and are performed.				
ISO27001	8.9	Configuration Management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed	To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes		Secure Configuration	Data Protection	This control is necessary for management control to monitor and measure adherence to standard security management practices as well as assurance that the integrity of the service assets and configuration items are protected. Additionally, the selection is to ensure technical compliance are reviewed to assess the level of compliance with policies, standards and other applicable regulations and are performed.	Yes	Yes	Yes	Yes
ISO27001	8.10	Information Deletion	Information stored in information systems and devices should be deleted when no longer required	To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for data deletion		Information Protection	Data Protection	It is required to ensure that records, irrespective of the format or medium thereof, that are received or created by BCX in the performance of its functions and in the execution of its business activities, are managed in such a manner that promotes good governance and compliance with	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
								applicable legislation.				
ISO27001	8.11	Data Masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and business requirement, taking legal requirements into consideration	To limit the exposure of sensitive data including personally identifiable information, and to comply with legal, statutory, regulatory and contractual requirements.		Information Protection	Data Protection	It is required to ensure any external/internal communication to and from the Cloud environment is subject to encryption controls across the boundaries to comply with relevant regulations, legislation and agreements. Cryptographic Controls should be in place where required when Asset Information is stored, processed and transported on Personnel Computers, USB devices or External devices.	Yes	Yes	Yes	Yes
ISO27001	8.12	Data Leakage Prevention	Data leakage prevention measures should be applied to systems, networks and endpoint devices that process, store or transmit sensitive information	To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems		Information Protection	Data Protection	This is required to emphasize the importance of protecting data generated, accessed, modified, disclosed, transmitted, destructed, and stored by the organisation, to identify procedures that should be in place to protect the confidentiality, integrity, and availability of data, and to comply with all regulations regarding privacy and confidentiality of information.	Yes	Yes	Yes	Yes
ISO27001	8.13	Information Backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with	To enable recovery from loss of data or systems		Continuity	Data Protection	This is required to ensure data backup of customers and support data, including critical system required for service delivery. This is also to ensure	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			the agreed topic-specific policy on backup					service restoration in the event of a disaster.				
ISO27001	8.14	Redundancy of Information Processing Facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	To ensure the continuous operation of information processing facilities		Continuity	Data Protection	This control is adopted to ensure availability of information processing facilities is made part of BCP process.	Yes	Yes	Yes	Yes
ISO27001	8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, protected, stored and analysed	To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations		Information Security Event Management	Security Incident Management	User activities and security event logs on Systems Databases and Application is required to be logged, stored and provided for future evidence as and when needed. Unauthorised access and alteration of data logs are prevented. This is required to ensure that privileged activities for Database administration are logged and monitored to prevent misuse.	Yes	Yes	Yes	Yes
ISO27001	8.16	Monitoring Activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	To detect anomalous behaviour and potential information security incidents		Information Security Event Management	Security Incident Management	Managing threats and vulnerabilities associated with business applications, systems and networks by: scanning for technical vulnerabilities; maintaining up-to-date patch levels; performing continuous security event monitoring; acting on threat intelligence; and protecting information against targeted cyber-attack	Yes	Yes	Yes	In planning

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
ISO27001	8.17	Clock Synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources	To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents		Information Security Event Management	Security Incident Management	Clock synchronization is required between all systems to ensure audit trail time snap shots are accurate	Yes	Yes	Yes	Yes
ISO27001	8.18	Use of Privileged Utility Programs	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled	To ensure the use of utility programs does not harm system and application controls for information security		System and Network Security	Data Protection	Ansible scripting is used to assist with the deployment of specific changes. This is done in a controlled manner.	Yes	Yes	Not Applicable	
ISO27001	8.19	Installation of Software on Operational Systems	Procedures and measures should be implemented to securely manage software installation on operational systems	To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.		Secure Configuration	End Point Security	Client system hosts software installation is configured as part of client system Take ON and during Operational/ Maintain/Support Software installations must be done in a controlled manner. BCX does not install Software on Client Workstations Client software in customer site are maintained and managed by Customer.	Yes	Yes	Not Applicable	
ISO27001	8.20	Network Controls	Networks should be managed and controlled to protect information in systems and applications	To ensure the protection of information in networks and its supporting information processing facilities		System and Network Security	Network Security	Client network environment network are designed and managed as per Client requirements. Internal network is provided managed as per policy	Yes	Yes	Yes	Yes
ISO27001	8.21	Security of Network Services	Security mechanisms, service levels, and service requirements of network services should be identified, implemented and monitored.	To ensure security in the use of network services		System and Network Security	Network Security	Client network environment network are designed and managed as per Client requirements. Internal network is provided managed as per policy	Yes	Yes	Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
ISO27001	8.22	Web Filtering	Access to external websites should be managed to reduce exposure to malicious content	To protect systems from being compromised by malware and to prevent access to unauthorized web resources		System and Network Security	Network Security	This is required to enforce the establishment of web filtering controls protect employees from accessing external websites that may contain viruses, phishing materials, or other types of illegal information.	Yes	Yes	Yes	Yes
ISO27001	8.23	Segregation in Networks	Groups of information services, users, and information systems should be segregated in the organization's networks	To split the network in security boundaries and to control traffic between them based on business needs		System and Network Security	Network Security	Client network environment network are designed and managed as per Client requirements. Internal network is provided managed as per policy	Yes	Yes	Yes	Yes
ISO27001	8.24	Use of Cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information in compliance with legal, statutory, regulatory or contractual requirements related to cryptography		Secure Configuration	Data Protection	Cryptography policy provides direction on how customer digital certificates are managed to ensure security requirements are met. This controls ensures that customer digital keys for Cloud Platforms are generated, exchanged, stored, used, destroyed and recovered securely in accordance with policy.	Yes	Yes	Yes	Yes
ISO27001	8.25	Secure Development Lifecycle	Rules for the secure development of software and systems should be established and applied	To ensure information security is designed and implemented within the secure development lifecycle of software and systems		System and Network Security	Data Protection	Rules should be established and applied to development of software and systems. This is also true for the development of new products or services in the Cloud and Infrastructure environment	Yes	Yes	Yes	Yes
ISO27001	8.26	Application Security Requirements	Information security requirements should be identified,	To ensure all information security requirements are identified and		Application Security	Data Protection	Passing of information across public networks via Field Metrix and customer integration	Yes	Yes	Yes	

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			specified and approved when developing or acquiring applications	addressed when developing or acquiring applications				services BCX Only Host Cloud Infrastructure and should protect Information involved in Service Transactions. Client network environment network are designed and managed as per Client partner architecture design requirements.				
ISO27001	8.27	Secure System Architecture and Engineering Principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities	To ensure information systems are securely designed, implemented and operated within the development lifecycle		System and Network Security	Data Protection	Required to ensure secure systems engineering principles are included into the Cloud solution through a secure architecture design and implementation	Yes		Yes	Yes
ISO27001	8.28	Secure Coding	Secure coding principles should be applied to software development	To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software		System and Network Security	Data Protection	BCX does not develop code on their platform	Not Applicable		Not Applicable	
ISO27001	8.29	Security Testing in Development and Acceptance	Security testing processes should be defined and implemented in the development lifecycle.	To validate if information security requirements are met when deployed to the production environment		Information Security Assurance	Security Compliance Management	Tests of security functionality should be carried out during development as is the case with the BCX One Cloud enviornment. Acceptance tests form part of the Project Management close out process for all new or changed information systems.	Yes	Yes	Yes	Yes
ISO27001	8.30	Outsourced Development	The organization should direct, monitor and review the activities related to outsourced	To ensure information security measures required by the organization are implemented in		Supplier Relationships Security	3rd Party Security	No external development is performed within this scope.	Not Applicable		Not Applicable	

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			system development	outsourced system development								
ISO27001	8.31	Separation of Development, Test and Production Environments	Development, testing, and production environments should be separated and secured	To protect the production environment and data from compromise by development and test activities		System and Network Security	Data Protection	Development environments of which BCX One Cloud is currently included should be secured and protected for integration and development.	Yes	Yes	Yes	Yes
ISO27001	8.32	Change Management	Changes to information processing facilities and information systems should be subject to change management procedures	To preserve information security when executing changes		System and Network Security	Data Protection	Change Management processes should be followed to consider risks to processes and systems and ensure availability of systems as per customer contracts. This change control process is being followed by means of logging a request to the IT Service desk. The change control process is then initiated via the assigned group. The change is also submitted to the customers change control process if there is customer impact. Testing is being performed to confirm the changes are implemented correctly and has no impact. Impact of changes are provided to customer. Where impact is unknown testing is required and done. FieldMetrix an external partner who hosts the application will periodically send us updated to the SDK	Yes	Yes	Yes	Yes
ISO27001	8.33	Test Information	Test information should be	To ensure relevance of		Information Protection	Data Protection	BCX does not test customer information	Not Applicable	No	Not Applicable	No

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			appropriately selected, protected and managed	testing and protection of operational information used for testing				and has no access to it.				
ISO27001	8.34	Protection of Information Systems during Audit and Testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management	To minimize the impact of audit and other assurance activities on operational systems and business processes.		Information Protection	Data Protection	This control ensures that operational system audits is performed in a manner to reduce any disruptions to customer business processes.	Yes		Yes	Yes
		ISO 27017 Controls										
ISO27017	CLD 6.3.1	Shared Roles and Responsibilities within a Cloud Computing Environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.	To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.		Governance	Access Governance	Information Security roles are defined in SLAs and MSAs with the customer.			Yes	Yes
ISO27017	CLD 8.1.5	Removal of Cloud Service Customer Assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	To identify organizational assets and define appropriate protection responsibilities.		Asset Management	Access Governance	Information assets contained in the cloud environment is removed or returned as per agreement with the customer. This includes data backups.			Yes	Yes
ISO27017	CLD 9.5.1	Segregation of Virtual Computing Environments	A cloud service customer's virtual environment running on a	To mitigate information security risks when using the shared virtual		Secure Configuration	Access Governance	Cloud customer environments should be segregated for information security and to minimise			Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			cloud service should be protected from other cloud service customers and unauthorized persons.	environment of cloud computing.				vulnerability or access to other information assets.				
ISO27017	CLD 9.5.2	Virtual Machine Hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.	To mitigate information security risks when using the shared virtual environment of cloud computing.		Secure Configuration	Access Governance	Virtual machines are utilised within BCX and hardened according to customer requirements or as per best practices.			Yes	Yes
ISO27017	CLD 12.1.5	Administrator's Operational Security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.	To ensure correct and secure operations of information processing facilities.		Governance	Access Governance	Administrative operations should be documented and monitored to ensure that only the necessary people can perform these actions and that adminstrators are managed, removed or added as per the documented procedures.			Yes	Yes
ISO27017	CLD 12.4.5	Monitoring of Cloud Services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	To record events and generate evidence.		Information Security Event Management	Security Incident Management	Customers within the BCX cloud environment should have monitoring capabililties as agreed in the MSA/SLAs			Yes	Yes
ISO27017	CLD 13.1.4	Alignment of Security Management for Virtual and Physical Networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.	To ensure the protection of information in networks and its supporting information processing facilities.		System and Network Security	Network Security	Consistency of configurations in the BCX cloud environment should be verified against the network security policy and the cloud design documentation.			Yes	Yes
		ISO 27018 Controls										

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
ISO 27018	A.1	Consent and choice										
ISO 27018	A.1.1	Obligation to co-operate regarding PII principals' rights	The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.				Data Protection	By law BCX is required to comply with POPIA requirements.			Yes	Yes
ISO 27018	A.2	Purpose legitimacy and specification										
ISO 27018	A2.1	Public cloud PII processor's purpose	PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.				Data Protection	By law BCX is required to comply with POPIA requirements. This is also a contractual requirement from cloud service customers.			Yes	Yes
ISO 27018	A.2.2	Public cloud PII processor's commercial use	PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.				Data Protection	By law BCX is required to comply with POPIA requirements. This is also a contractual requirement from cloud service customers.			Yes	Yes
ISO 27018	A.3	Collection limitation										
ISO 27018			No additional controls				Data Protection				Yes	Yes
ISO 27018	A.4	Data minimization										

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
ISO 27018	A.4.1	Secure erasure of temporary files	Temporary files and documents should be erased or destroyed within a specified, documented period.				Data Protection	Temporary files may contain PII and might be used to reconstruct information.			Yes	Yes
ISO 27018	A.5	Use, retention, and disclosure limitation										
ISO 27018	A.5.1	PII disclosure notification	The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.				Data Protection	BCX is required by law ot notify the customer of disclosures of PII			Yes	Yes
ISO 27018	A.5.2	Recording of PII disclosures	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.				Data Protection	It is the responsibility of BCX to ensure that disclosures of PII to third parties is recorded. Should this PII become available there should be evidence to prove that PII was handled according to policy and the terms and conditions related to the disclosure. During audits information could also be disclosed during the			Yes	

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
								normal course of operations.				
ISO 27018	A.7	Openness, Transparency and Notice										
ISO 27018	A.7.1	Disclosure of sub-contracted PII processing	The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.				Data Protection	BCX makes use of suppliers to provide the cloud services.			Yes	Yes
ISO 27018	A.9	Accountability										
ISO 27018	A.9.1	Notification of a data breach involving PII	The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.				Data Protection	BCX is required by law to notify the customer of data breaches.			Yes	Yes
ISO 27018	A.9.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).				Data Protection	Policies and procedures may be involved during dispute resolution and investigations.			Yes	Yes
ISO 27018	A.9.3	PII return, transfer and disposal	The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy				Data Protection	The customer has the right to PII as per the POPIA act.			Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			available to the cloud service customer.									
ISO 27018	A.10	Information Security										
ISO 27018	A.10.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.				Data Protection	POPIA Act requirements.			Yes	Yes
ISO 27018	A.10.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted.				Malware Protection	The BCX Data Classification Policy includes rules about hardcopy materials related to PII.			Yes	Yes
ISO 27018	A.10.3	Control and logging of data restoration	There should be a procedure for, and a log of, data restoration efforts.				Data Protection	BCX has a Backup Policy in place for Datacentres			Yes	Yes
ISO 27018	A.10.4	Protecting data on storage media leaving the premises	PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).				Data Protection	Data should be protected on storage media leaving the premises as this will have contractual implications and POPIA requirements.			Yes	Yes
ISO 27018	A.10.5	Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.				Data Protection				Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
ISO 27018	A.10.6	Encryption of PII transmitted over public data-transmission networks	PII that is transmitted over public data transmission networks should be encrypted prior to transmission.				Data Protection	This forms part of the BCX Cloud Service Design			Yes	Yes
ISO 27018	A.10.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.				Data Protection	POPIA Act and BCX Data Retention and Destruction Policy requirements.			Yes	Yes
ISO 27018	A.10.8	Unique use of user IDs	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.				Data Protection	BCX ICT Services Policy and Acceptable Use Policies			Yes	Yes
ISO 27018	A.10.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.				Data Protection	BCX ICT Services Policy and Acceptable Use Policies			Yes	Yes
ISO 27018	A.10.10	User ID management	De-activated or expired user IDs should not be granted to other individuals.				Data Protection	This control is required to ensure traceability for audit or evidence purposes.			Yes	Yes
	A.10.11	Contract measures	Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational				Data Protection	It is a requirement of POPIA.			Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.									
	A.10.12	Sub-contracted PII processing	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.				Data Protection	POPIA Requirement			Yes	Yes
	A.10.13	Access to data on pre-used data storage space	The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that				Data Protection	Data should only be available to the relevant customer and not be visible to others on the shared cloud fabric			Yes	Yes

ISO Standard	ISO Control Number	Control Title	Control Description	Control Purpose	Cybersecurity Concepts	Operational Capabilities	BCX Security Domains	Reason for Inclusion / Exclusion	Applicability across BCX	Implemented for BCX	Applicability Cloud Platforms	Implemented for Cloud Platforms
			cloud service customer.									
	A.11	**Privacy compliance**										
ISO27018	A.11.1	Geographical location of PII	The public cloud PII processor should specify and document the countries in which PII might possibly be stored.				Data Protection	The locations of the cloud service PII should be stored as it is a service offering and part of the ISO certification process of BCX			Yes	Yes
ISO27018	A.11.2	Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.				Data Protection	POPIA and contractual obligations.			Yes	Yes