STATEMENT OF APPLICABILITY - HCL Software SOA

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Applicability	Implemented control/s	Comment / Justication for exclusion
A.5	**Security Policy**			
A.5.1	**Management direction for information security**			
A.5.1.1	Policies for Information Security –A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System	HCL Software security programs is established through formal documented requirements that include HCL Software Security Policies, HCL Privacy Statement, HCL Corporate policies and Code of Business Ethics and Conduct
A.5.1.2	Review of the policies for Information Security – The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System	HCL Software and HCL Corporate has policies in place and reviews them at least annually to ensure relevance.
A.6	**Organization of information Security**			
A.6.1	**Internal Organization**			
A.6.1.1	Information Security roles and responsibilities– All information security responsibilities shall be defined and allocated.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software follows Instruction that requires roles and responsibilities and Separation of Duties across multiple policies	HCL Software has roles and responsibilities defined, delegations of duty and restrictions on access throughout its policies.
A.6.1.2	Segregation of duties- Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software operate permissions systems, least needs access throughout its policies to ensure separation of duties	HCL Software follows Instruction that requires Separation of Duties by ensuring that no one individual has two or more responsibilities or accesses that would allow them to misuse or divert company assets. Product teams are responsible for ensuring adequate Separation of Duties exists within its organization.
A.6.1.3	Contact with authorities- Appropriate contacts with relevant authorities shall be maintained.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System and its Incident Management policy	HCL has identified resources to handle contact with authorities.
A.6.1.4	Contact with special interest groups - Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	Various Policies & Products relate to areas of special interest	HCL Products and Platform Specific teams have special interests
A.6.1.5	Information Security in Project Management- Information security shall be addressed in project management, regardless of the type of the project.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Secure Engineering Practices governed by our Development and Maintenance policies and Release Management Practices	Secure Engineering Practices provides guidelines on Project Planning for Security Practice Area. All released product must comply with specific enhanced security requirements prior to release.
A.6.2	**Mobile devices and Teleworking**			
A.6.2.1	Mobile Device Policy- A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Security and Standards for all Employees includes security measures for mobile devices	HCL Software maintains mandatory compliance criteria for workstations and mobile devices within HCL Security Use Standards for Employees.

A.6.2.2	Teleworking- A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Security and Standards for all Employees includes security measures for teleworking / remote working	HCL Software Security and Standards for all Employees includes security measures for teleworking / remote working
A.7	**Human Resources security**			
A.7.1	**Prior to employment**			
A.7.1.1	Screening - Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Human Resource practices	HCL performs background checks on all new employees through HCL Recruitment practices
A.7.1.2	Terms and conditions of employment -The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System, Human Resource Practices and Code of Business Ethics and Conduct	Employees are required to enter into confidentiality agreements and adhere to the HCL Code of Business Ethics and Conduct
A.7.2	**During employment**			
A.7.2.1	Management Responsibilities - Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System, Human Resource Practices and Code of Business Ethics and Conduct	All HCL Software managers must ensure that their employees adhere to HCL Software security requirements for the data and IT resources within their area of responsibility. Managers are also responsible to deny requests for unnecessary access to resources and to remove access to resources when they are no longer needed by employees. Employment Verification must be in place for annual employment verification of individuals assigned a userid on internal HCL Software systems.
A.7.2.2	Information security awareness, education and training – All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	Mandatory Information Security Annual Training, Code of Business Ethics and Conduct and various Security Policies	Employees are required to complete information security training annually. Progress is communicated to managers via automated emails/tools/reports and tracked to completion.
A.7.2.3	Disciplinary Process - There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System, Human Resource Practices and Code of Business Ethics and Conduct	Employees must at all times comply with Code of Business Ethics and Conduct related guidelines. Violation of any HCL guideline is cause for discipline including dismissal from the company, as stated in the Code of Business Ethics and Conduct.
A.7.3	**Termination or change of employment**			
A.7.3.1	Termination or change of employment responsibilities - Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System, HR Separation practice	All HCL Software managers must ensure appropriate removal or modification of access for employee termination or change of employment responsibility. Managers are also responsible to remove access to resources when they are no longer needed by employees. Employment Verification must be in place for annual employment verification of individuals assigned a userid on internal HCL Software systems.
A.8	**Asset management**			
A.8.1	**Responsibility for assets**			
A.8.1.1	Inventory of assets – Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy, tooling to support management of the inventory	HCL Software ISMS - Asset Management policy requires identifying and maintaining and Asset Inventory

A.8.1.2	Ownership of assets - Assets maintained in the inventory shall be owned.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy, tooling to support management of the inventory	Each asset maintained in the inventory must have an identified owner.
A.8.1.3	Acceptable use of assets - Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy, Code of Business Ethics and Conduct	HCL Software maintains acceptable use criteria within HCL Software ISMS - Asset Management policy. Additionally, it's Code of Business Ethics and Conduct defines the HCL code of conduct and addresses the issues of, but is not limited to, (1) rules for fair and appropriate dealings with our customers, competitors, the general public and fellow HCL staff; (2) acquisition and handling of information about others or owned by others and receiving information that may be confidential or has restrictions on its use; (3) rules regarding protection of customer-owned data, i.e., that all customer-owned data should be protected.
A.8.1.4	Return of assets - All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Human Resource practices, HR Separation practice	HCL HR has processes and procedures which address return of assets from terminated employees.
A.8.2	**Information Classification**			
A.8.2.1	Classifications of Information - Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy, HCL Data Classification Policy	Information must be classified in terms of our Information and Data Classification policies.
A.8.2.2	Labelling of information – An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy	Information must be labelled based on classification in terms of our Information and Data Classification policies.
A.8.2.3	Handling of assets- Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy	Assets must be handled to ensure secure processing, storage, transmission, declassification and destruction also considering Information Classification and labelling
A.8.3	**Media Handling**			
A.8.3.1	Management of removable media- Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy	HCL Software seldom manage/use removable media. However, if we do, Information Owners / Custodians must ensure the management of removable media in accordance with the information classification. Cryptographic techniques must be used to protect data on all removable media. Authorization must be required and documented for media removed from the organization. If no longer required, the contents of any re-usable media that are to be removed from the organization must be made unrecoverable.

A.8.3.2	Disposal of media- Media shall be disposed of securely when no longer required, using formal procedures.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy	HCL Software seldom manage/use removable media. However, if we do, Information Owners / Custodians must ensure the management of removable media in accordance with the information classification. Cryptographic techniques must be used to protect data on all removable media. Authorization must be required and documented for media removed from the organization. If no longer required, the contents of any re-usable media that are to be removed from the organization must be made unrecoverable.
A.8.3.3	Physical media transfer- Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management policy	HCL Software seldom manage/use removable media. However, if we do, Information Owners / Custodians must ensure the management of removable media in accordance with the information classification. Cryptographic techniques must be used to protect data on all removable media. Authorization must be required and documented for media removed from the organization. If no longer required, the contents of any re-usable media that are to be removed from the organization must be made unrecoverable.
A.9	**Access Control**			
A.9.1	**Business Requirement for Access Control**			
A.9.1.1	Access Control Policy – An access control policy shall be established, documented and reviewed based on business and security requirements for access.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	HCL Software Access Control policy requires access controls have elements of need to know basis, least privilege and management support included in Identification, Authorization, System and security administrative authority, Access authorization, and Application security administrative authority requirements
A.9.1.2	Access to networks and network services- Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	HCL Software Access Control policy defines standards for Identification, Authentication and Authorization for network devices.
A.9.2	**User Access Management**			
A.9.2.1	User Registration and deregistration– A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	User registration and de-registration standards are defined in HCL Software Access Control policy. The controls include Information Owner approvals, specific requirements and time frames.
A.9.2.2	User access provisioning - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	Requirements and management of privileged access controls are defined in HCL Software Access Control policy
A.9.2.3	Management of privileged access rights- The allocation and use of privileged access rights shall be restricted and controlled.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	Management of privileged access requires management approval and regular reviews as defined in HCL Software Access Control policy.
A.9.2.4	Management of secret authentication information of users - The allocation of secret authentication information shall be controlled through a formal management process.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy, Code of Business Ethics and Conduct and Information Security Training	HCL Software requires mechanisms for protecting password information when in use or being renewed as defined in HCL Software Access Control policy.

A.9.2.5	Review of User Access Rights – Management shall review users access rights at regular intervals using a formal process	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	Regular reviews by management of user access consists of Employee verification, Continued business need, Privileged access review as defined in the HCL Software Access Control policy
A.9.2.6	Removal or adjustment of access rights - The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy, HCL Human Resource practices, HR Separation practice	HCL Software Access Control policy includes policy for revoking userids and for employment termination, verification and continued business need.
A.9.3	**User Responsibilities**			
A.9.3.1	Use of secret authentication information - Users shall be required to follow the organization’s practices in the use of secret authentication information.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	HCL Software ISMS - Access Controls policy contains details for management of secret authentication details including the mechanisms for protecting password information and a process for creating strong passwords.
A.9.4	**System and application access control**			
A.9.4.1	Information access restriction - Access to information and application system functions shall be restricted in accordance with the access control policy.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	HCL Software Access control requirements are defined at both system- and application-levels.
A.9.4.2	Secure log-on procedures - Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	HCL Software Production delivery treats all system, application and data as confidential unless specifically exempted and therefore any log on access must be secure log-on
A.9.4.3	Password management system - Password management systems shall be interactive and shall ensure quality passwords.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	HCL Software ISMS - Access Controls policy contains details for management of secret authentication details including the mechanisms for protecting password information and a process for creating strong passwords.
A.9.4.4	Use of privileged utility programs - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	HCL Software access for utility programs is defined by the requirements in the Access Control policy.
A.9.4.5	Access control to program source code- Access to program source code shall be restricted.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Access Controls policy	Processes for modifying software as authorized by HCL Software management are defined in HCL Software Access Control policy.
A.10	**Cryptography**			
A.10.1	**Cryptographic controls**			
A.10.1.1	Policy on the use of cryptographic controls - A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Cryptography policy	Encryption is required for data at rest and in transit.
A.10.1.2	Key management - A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Cryptography policy	A policy on the use, protection and lifetime of cryptographic keys has be developed and implemented through their whole lifecycle.
A.11	**Physical and environmental security**			
A.11.1	**Secure areas**			

A.11.1.1	Physical security perimeter – Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes perimeter security for HCL data centers. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.1.2	Physical entry controls – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes entry control security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.1.3	Securing offices, rooms and facilities – Physical security for offices, rooms and facilities shall be designed and applied	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes entry control security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.1.4	Protecting against external and environmental threats - Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster shall be designed and applied.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes external and environmental security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.1.5	Working in secure areas - Physical protection and guidelines for working in secure areas shall be designed and applied.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes policy for working in secure areas for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.1.6	Delivery and loading areas - Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and if possible isolated from information processing facilities to avoid unauthorized access	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes Delivery and loading area security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2	**Equipment**			
A.11.2.1	Equipment siting and protection – Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes siting and protection security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2.2	Supporting utilities - Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes supporting utilities security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2.3	Cabling Security – Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes cabling security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.

A.11.2.4	Equipment maintenance – Equipment shall be correctly maintained to ensure its continued availability	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes equipment maintenance security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2.5	Removal of assets - Equipment, information or software shall not be taken off-site without prior authorization.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security, HCL Software ISMS - Asset Management	HCL Software Physical and Environmental Security and HCL Software Asset Management describe removal of assets security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2.6	Security of equipment and assets off-premises – Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security	HCL Software Physical and Environmental Security describes equipment and asset off-premise security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2.7	Secure disposal or re-use of equipment – All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Physical and Environmental Security, HCL Software ISMS - Asset Management	HCL Software Physical and Environmental Security and HCL Software Asset Management describe disposal and re-use security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2.8	Unattended user equipment - Users shall ensure that unattended equipment has appropriate protection.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Human Resources	HCL Software Human Resource policy describes clean desk and clear screen (including Unattended equipment) security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.11.2.9	Clear desk and clear screen policy - A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Human Resources	HCL Software Human Resource policy describes clean desk and clear screen security for HCL data centers and development environments. For Physical controls that are implemented by data centers outside of HCL, the HCL Software Physical and Environmental Security policy is used as guidelines.
A.12	**Operations Security**			
A.12.1	**Operational procedures and responsibilities**			
A.12.1.1	Documented operating procedures – Operating procedures shall be documented, maintained and made available to all users who need them.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Operational Security	HCL Software security practices are established through formal documented requirements for operational security activities
A.12.1.2	Change Management - Changes to information processing facilities and systems shall be controlled.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS	Changes to the organization, security policy and any processes / procedure that affect information security should be controlled.
A.12.1.3	Capacity Management – The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning HCL Software ISMS - Health Check of Environments	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning provides requirements of capacity planning / projection and HCL Software Health Check policy has capacity management as a health check requirement for monitoring

A.12.1.4	Separation of development, testing and operational environments – Development and testing facilities shall be separated from operational facilities. Rules for the migration of the software from the development to operational status needs to be defined and documented.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMA - System Acquisition, Development and Maintenance policy	HCL Software practice secure engineering including separation for development and test activities
A.12.2	**Protection from malware**			
A.12.2.1	Controls against malware- Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning	HCL Software approved anti-virus program/solution to detect and block malware being uploaded is a requirement for any device to be security ready
A.12.3	**Back up**			
A.12.3.1	Information back up- Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software secures daily and weekly backups which are encrypted and stored.
A.12.4	**Logging and Monitoring**			
A.12.4.1	Event Logging - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Security Monitoring and Logging	HCL Software security strategy includes the requirement to establish standard methods of recording various security related activity through event logging.
A.12.4.2	Protection of log information - Logging facilities and log information shall be protected against tampering and unauthorized access	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Security Monitoring and Logging	Access to log information is controlled to prevent any tampering or unauthorised access
A.12.4.3	Administrator and operator logs - System administrator and system operator activities shall be logged.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Security Monitoring and Logging	Administrator and operator logs shall be logged and the policy is to ensure this level of logging is never disabled.
A.12.4.4	Clock synchronization - The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning	Clock Synchronisation as a security readiness requirement for all devices ensures that activity logging has synchronized timings.
A.12.5	**Control of operational software**			
A.12.5.1	Installation of software on operational systems - Procedures shall be implemented to control the installation of software on operational systems.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance, HCL Software ISMS - Security Readiness Standard, Provisioning and Deprovisioning and HCL Software ISMS - Patch Management	HCL practices for software deployment, device readiness and patch management assure the controls required for software installation and management on operating systems
A.12.6	**Technical vulnerability management**			
A.12.6.1	Management of technical vulnerabilities - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Vulnerability Scanning	Initial service activation vulnerability scans and periodic scans must be performed. Upon identification of potential technical vulnerabilities, corrective action must be taken to an established time-line. Vulnerability scanning - TCP/IP vulnerability scanning must be conducted. Security advisory patch management to install security advisory patches within the time limits outlined.

A.12.6.2	Restrictions on software installation - Rules governing the installation of software by users shall be established and implemented.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Asset Management and HCL Code of Business Ethics and Conduct	Software installations must adhere to HCL Acceptable Use policy and our Code of Business Ethics and Conduct. Software must only be used in accordance with contract agreements and copyright laws.
A.12.7	**Information systems audit considerations**			
A.12.7.1	Information systems audit controls - Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Health Check of Environments and HCL Software ISMS - Internal Audit and Compliance	Health checking across all environments provides and audit of environment status against our health check criteria. Internal Audit provides assurance of compliance to all aspects of our ISMS
A.13	**Communications Security**			
A.13.1	**Network security management**			
A.13.1.1	Network Controls – Networks shall be managed and controlled to protect information in systems and applications.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Communication Controls (Networks & Firewalls)	HCL Software data network infrastructure must meet our security requirements to preserve the security of data and data in motion across our offerings. Our Policy provides the guidance for the management and control of networks, network devices or applications that provide Network Services .
A.13.1.2	Security of network services - Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Communication Controls (Networks & Firewalls)	HCL Software data network infrastructure must meet our security requirements to preserve the security of data and data in motion across our offerings. Our Policy provides the guidance for the management and control of networks, network devices or applications that provide Network Services .
A.13.1.3	Segregation in Networks – Groups of information services users and information systems shall be segregated on networks	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Communication Controls (Networks & Firewalls)	HCL Software data network infrastructure must meet our security requirements to preserve the security of data and data in motion across our offerings. Our Policy provides the guidance for the management and control of networks, network devices or applications that provide Network Services .
A.13.2	**Information Transfer**			
A.13.2.1	Information transfer policies and procedures - Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Human Resources, HCL Code of Business Ethics and Conduct and HCL Software ISMS - Cryptography	HCL Software employees should neither receive from nor disclose to any other party any Confidential Information (as per our Code of Business Ethics and Conduct) without following procedures. All data in transit is encrypted for protections.
A.13.2.2	Agreements on information transfer- Agreements shall address the secure transfer of business information between the organization and external parties.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Supplier Management	HCL Software supplier agreements include security controls on data transfer. Information is never shared without a Non Disclosure agreement in place.
A.13.2.3	Electronic messaging - Information involved in electronic messaging shall be appropriately protected.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Human Resources, HCL Code of Business Ethics and Conduct and HCL corporate email standards	Based on information classification, private/confidential information is not disclosed to unauthorized individuals during electronic transmission.
A.13.2.4	Confidentiality or non-disclosure agreements- Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, regularly reviewed and documented.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Supplier Management, HCL Software ISMS - Human Resources, HCL Code of Business Ethics and Conduct and HCL Software ISMS - Cryptography	HCL Software supplier agreements include security controls on data transfer. Information is never shared without a Non Disclosure agreement in place. This approach is supported by our HR and Code of Business Ethics and Conduct policies
A.14	**System acquisition, development and maintenance**			
A.14.1	**Security requirements of information systems**			

A.14.1.1	Information security requirements analysis and specification - The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	All information security requirements are included at the time of acquisition, development and maintenance of systems and products
A.14.1.2	Securing application services on public networks - Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy and HCL Software ISMS - Cryptography	Requirement to protect information are assessed, protective solutions applied and all information passing over public networks shall be encrypted
A.14.1.3	Protecting application services transactions - Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorized disclosure, unauthorized message duplication or replay.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy and HCL Software ISMS - Cryptography	Requirement to protect service transactions are assessed, protective solutions applied and all information passing over public networks shall be encrypted
A.14.2	**Security in development and support processes**			
A.14.2.1	Secure development policy - Rules for the development of software and systems shall be established and applied to developments within the organization.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices
A.14.2.2	System change control procedures - Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including formal change controls
A.14.2.3	Technical review of applications after operating platform changes - When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including verification and validation after operating system changes
A.14.2.4	Restrictions on changes to software packages - Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including consideration on restricting changes
A.14.2.5	Secure system engineering principles - Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices
A.14.2.6	Secure development environment - Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including development environments
A.14.2.7	Outsourced development - The organization shall supervise and monitor the activity of outsourced system development.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	HCL Software does not currently outsource development. If it does in the future, we have a policy and controls to consider before commencing any outsource agreement

A.14.2.8	System security testing - Testing of security functionality shall be carried out during development.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including system security testing
A.14.2.9	System acceptance testing - Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including system acceptance testing
A.14.3	**Test Data**			
A.14.3.1	Protection of test data- Test data shall be selected carefully, protected and controlled.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - System Acquisition, Development and Maintenance policy	Secure Engineering principles are applied to development practices including protection of test data
A.15	**Supplier relationships**			
A.15.1	**Information security in supplier relationships**			
A.15.1.1	Information security policy for supplier relationships - Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Supplier Management	Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.15.1.2	Addressing security within supplier agreements - All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Supplier Management	Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.15.1.3	Information and communication technology supply chain - Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Supplier Management	Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.15.2	**Supplier service delivery management**			
A.15.2.1	Monitoring and review of supplier services - Organizations shall regularly monitor, review and audit supplier service delivery.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Supplier Management	Performance Monitoring for Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to perform to a standards as defined by the HCL Software ISMS
A.15.2.2	Managing changes to supplier services - Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Supplier Management	Security requirements for the Supplier's are managed as part of any supplier agreement. HCL will expect as a minimum to match all security requirements and standards as defined by the HCL Software ISMS
A.16	**Information Security Incident Management**			
A.16.1	**Management of information security incidents and improvements**			
A.16.1.1	Responsibilities and procedures - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios. HCL Software's Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.

A.16.1.2	Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Incident Management	For security Incidents that may occur, product teams work with HCL Software's Incident Response team and HCL Legal to address incidents involving loss or exposure of PI Data. HCL Software’s Incident Response team includes a group that has a data incident response process which supports all of HCL operations 24x7x365 worldwide.
A.16.1.3	Reporting security weaknesses - All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Incident Management and Information Security Training	HCL Software has a dedicated Incident Response team that focuses on various scenarios. HCL Software’s Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.16.1.4	Assessment of and decisions on information security events - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios. HCL Software’s Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.16.1.5	Response to information security incidents - Information security incidents shall be responded to in accordance with the documented procedures.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios. HCL Software’s Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.16.1.6	Learning from information security incidents - Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Incident Management	HCL Software perform incident analysis to learn from information security incidents and drive continued improvement
A.16.1.7	Collection of evidence - The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Incident Management	HCL Software has a dedicated Incident Response team that focuses on various scenarios and including the collection of evidence. HCL Software’s Incident Response team includes a group that has a data incident response process which supports all of HCL Software operations 24x7x365 worldwide.
A.17	**Information security aspects of business continuity management**			
A.17.1	**Information security continuity**			
A.17.1.1	Planning information security continuity- The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software have a formal approach to planning for information security continuity
A.17.1.2	Implementing information security continuity - The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software have a formal approach to planning for information security continuity
A.17.1.3	Verify, review and evaluate information security continuity - The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software have a formal approach to planning for information security continuity
A.17.2	**Redundancies**			
A.17.2.1	Availability of information processing facilities - Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Information Security Aspects of Business Continuity	HCL Software have a formal approach to planning for information security continuity

A.18	**Compliance**			
A.18.1	**Compliance with legal and contractual requirements**			
A.18.1.1	Identification of applicable legislation and contractual requirements - All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	Corporate Instructions: HCL legal & Regulatory	Corporate instructions mandate management of these processes via the Regulatory team. Legal provides all guidance on legal and contractual requirements.
A.18.1.2	Intellectual Property Rights (IPR) – Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software - Release Management, Certificate of Originality	Corporate Instructions on Intellectual Property include Rights to Intellectual Property, Invention protection, Receipt and Disclosure of confidential information, Patents and Inventions, Product and services reviews, copying of published materials, examination of non-HCL software.
A.18.1.3	Protection of records - Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software Information Security Management System (tools), HCL Software ISMS - Access Controls, HCL Human Resource Practices and Code of Business Ethics and Conduct	Tooling used in support of the HCL Software ISMS is access controlled and designed to protect all records / data. All employees contracts include details regarding Confidential Information, Intellectual Property, and Other Matter
A.18.1.4	Privacy and protection of personally identifiable information - Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Corporate - Privacy Statement	HCL Software Privacy and protection of personally identifiable controls are defined in our Privacy Statement supported by our classification and control of information
A.18.1.5	Regulation of cryptographic controls - Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Cryptography	Designed to meet requirements, encryption is required for data at rest and in transit. A policy on the use, protection and lifetime of cryptographic keys has be developed and implemented through their whole lifecycle.
A.18.2	**Information security reviews**			
A.18.2.1	Independent review of information security - The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Internal Audit and Compliance	HCL Software Internal Audit program and external independent auditors perform independent reviews of information security implementation and compliance.
A.18.2.2	Compliance with security policies and standards - Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Internal Audit and Compliance and all ISMS Operational Security activities	HCL Software Management is responsible for ensuring compliance with the policies and procedures and reviewing the compliance within their products. Security operational monitoring is conducted on an ongoing basis
A.18.2.3	Technical compliance review - Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	HCL Software Cloud HCL Multi-Products All Data Centres Product Support	HCL Software ISMS - Internal Audit and Compliance and all ISMS Operational Security activities	HCL Software Management is responsible for ensuring technical compliance with the requirements of the ISMS. Security operational monitoring is conducted on an ongoing basis giving insight to technical compliance