Keysight ISO 27001:2013 Statement of Applicability **rev - 1 February 2019**

Standard Clause or Control	Status	Justification
4.1 Understanding the organization and its context	Included	ISO Requirement
4.2 Understanding the needs and expectations of interested parties	Included	ISO Requirement
4.3 Determining the scope of the information security management system	Included	ISO Requirement
4.4 Information security management system	Included	ISO Requirement
5.1 Leadership and commitment	Included	ISO Requirement
5.2 Policy	Included	ISO Requirement
5.3 Organizational roles, responsibilities and authorities	Included	ISO Requirement
6.1.1 General actions to address risks and opportunities	Included	ISO Requirement
6.1.2 Information security risk assessment	Included	ISO Requirement
6.1.3 Information security risk treatment	Included	ISO Requirement
6.2 Information security objectives and planning to achieve them	Included	ISO Requirement
7.1 Resources	Included	ISO Requirement
7.2 Competence	Included	ISO Requirement
7.3 Awareness	Included	ISO Requirement
7.4 Communication	Included	ISO Requirement
7.5.1 General Documented Information	Included	ISO Requirement
7.5.2 Creating and updating	Included	ISO Requirement
7.5.3 Control of documented information	Included	ISO Requirement
8.1 Operational planning and control	Included	ISO Requirement
8.2 Information security risk assessment	Included	ISO Requirement
8.3 Information security risk	Included	ISO Requirement
9.1 Monitoring, measurement, analysis and evaluation	Included	ISO Requirement
9.2 Internal audit	Included	ISO Requirement
9.3 Management review	Included	ISO Requirement
10.1 Nonconformity and corrective action	Included	ISO Requirement
10.2 Continual improvement	Included	ISO Requirement
A.5.1.1 Policies for information security	Included	The ISMS is managed using controlled policies.
A.5.1.2 Review of the policies for information security	Included	Policies are reviewed.

A.6.1.1 Information security roles and responsibilities	Included	ISMS roles and responsibilities have been assigned.
A.6.1.2 Segregation of duties	Included	Organization segregates duties.
A.6.1.3 Contact with authorities	Included	Contacts with our defense related customers who have requirements for NIST 800-171 compliance and higher access controls for their CDI data.
A.6.1.4 Contact with special interest groups	Included	The acting ISMS Manager (among others) maintains membership in ISSA, SANS, and others.
A.6.1.5 Information security in project management	Included	Project Management uses the Project Charter to guide implementations.
A.6.2.1 Mobile device policy	Included	Relevant Keysight employees are provided with mobile devices.
A.6.2.2 Teleworking	Included	Acceptable Use Policy addresses teleworking and off-premise security.
A.7.1.1 Screening	Included	HR background-screens prospective employees. The background reports are held confidential. To verify, HR will have to request a compliance letter from the vendor and present it to the auditor.
A.7.1.2 Terms and conditions of employment	Included	Regarding information security, Keysight requires employees to sign the ARCIPD and Standards of Business Conduct, and stipulate to all Policies by signing the ARCIPD.
A.7.2.1 Management responsibilities	Included	All employees agree to abide by all policies in Point 7 of the ARCIPD.
A.7.2.2 Information security awareness, education and training	Included	Keysight uses an LMS, 'Wombat', to provide ISMS training and awareness.
A.7.2.3 Disciplinary process	Included	Requirements are put in place to terminate for IS breach.
A.7.3.1 Termination or change of employment responsibilities	Included	Users are deregistered on termination.
A.8.1.1 Inventory of assets	Included	Assets include servers, VMs, and workstations.
A.8.1.2 Ownership of assets	Included	All assets have a group owner.
A.8.1.3 Acceptable use of assets	Included	All employees acknowledge the Acceptable Use Policy by signing the ARCIPD.
A.8.1.4 Return of assets	Included	Managers are required to manage the asset return process for any of their own terminated employees.
A.8.2.1 Classification of information	Included	Information is classified as 'Private', then 'Confidential', then 'Restricted', then 'Public'.
A.8.2.2 Labelling of information	Included	Documents and electronic documents are labelled.
A.8.2.3 Handling of assets	Included	Workstations are protected by access control, the asset will only contain private/confidential information unless user has appropriate access level. Servers are higher risk and those assets are handled via physical key assignment.
A.8.3.1 Management of removable media	Included	Keysight does not provide removable media but employees may use theirs.
A.8.3.2 Disposal of media	Included	Media is securely disposed when it cannot be reused.

A.8.3.3 Physical media transfer	Included	Physical media transfer is exceedingly rare, but there are policies just in case.
A.9.1.1 Access control policy	Included	Access Control Policy is maintained.
A.9.1.2 Access to networks and network services	Included	Network access is controlled to protect Keysight IP.
A.9.2.1 User registration and de-registration	Included	Users are registered and de-registered.
A.9.2.2 User access provisioning	Included	Users are provisioned with different levels of IT access.
A.9.2.3 Management of privileged access rights	Included	Users are separated into groups; some are assigned admin rights based on competence and job function.
A.9.2.4 Management of secret authentication information of users	Included	Passwords are securely managed and stored.
A.9.2.5 Review of user access rights	Included	Managers are required to review access control rights for any of their own employees.
A.9.2.6 Removal or adjustment of access rights	Included	User access rights are removed at termination; if they return as a contractor they will be given separate domain access.
A.9.3.1 Use of secret authentication information	Included	Passwords are securely managed and stored.
A.9.4.1 Information access restriction	Included	The Access Control Policy is enforced.
A.9.4.2 Secure log-on procedures	Included	User logons are controlled and logged.
A.9.4.3 Password management system	Included	Keysight uses the Password manager built into Microsoft AD.
A.9.4.4 Use of privileged utility programs	Included	Identified utility program are Microsoft System Center Config Manager (SCCM), PowerBroker, and CyberArk. Access for each application is controlled within each group
A.9.4.5 Access control to program source code	**Excluded**	Software development is out of scope
A.10.1.1 Policy on the use of cryptographic controls	Included	Several types of cryptographic controls are in use, both in-transit and at-rest.
A.10.1.2 Key management	Included	Cryptographic keys/ web certificates are controlled and securely stored.
A.11.1.1 Physical security perimeter	Included	Badge in and security check required to enter any building.
A.11.1.2 Physical entry controls	Included	Badge in and security check required to enter any building.
A.11.1.3 Securing offices, rooms and facilities	Included	Functional areas within buildings require additional badging in.
A.11.1.4 Protecting against external and environmental threats	Included	Data center is almost 100% redundant, except that power feeds both come from the same utility. Redundant UPS, Generators, and HVAC.
A.11.1.5 Working in secure areas	Included	Secure areas require additional badging in. Secure servers require separate cabinet key.

A.11.1.6 Delivery and loading areas	Included	Delivery and loading only communicates with the general access area and not the data center itself. Delivery area is staffed.
A.11.2.1 Equipment siting and protection	Included	Surge protection and fire protection installed.
A.11.2.2 Supporting utilities	Included	Data center power supply is over 200% of typical load.
A.11.2.3 Cabling security	Included	Cables are accessible but overhead and only to staff approved to be in the secure area.
A.11.2.4 Equipment maintenance	Included	Supporting equipment is maintained. Servers are securely destroyed.
A.11.2.5 Removal of assets	Included	Asset removal is applicable only to the data center; all other assets are portable workstations.
A.11.2.6 Security of equipment and assets off-premises	Included	Acceptable Use Policy addresses teleworking and off-premise security.
A.11.2.7 Secure disposal or reuse of equipment	Included	If disposed, assets require a certificate of destruction. The only equipment reused are some workstations when employees leave. Workstation drives are encrypted and access managed with AD. Reimaging is all that is required. Even if not reimaged, new users will not be able to access the old data.
A.11.2.8 Unattended user equipment	Included	Acceptable Use Policy addresses unattended workstations/ clear desk and screen.
A.11.2.9 Clear desk and clear screen policy	Included	Acceptable Use Policy addresses unattended workstations/ clear desk and screen.
A.12.1.1 Documented operating procedures	Included	All functional towers have implemented operating procedures.
A.12.1.2 Change management	Included	Change management is handled by the HP ECMS System.
A.12.1.3 Capacity management	Included	Capacity management is performed by IS for the data center.
A.12.1.4 Separation of development, testing and operational environments	**Excluded**	Software development is out of scope
A.12.2.1 Controls against malware	Included	Each workstation and server includes malware protection.
A.12.3.1 Information backup	Included	The Colorado Springs Data Center has a redundant backup in Dallas. Critical systems are backed up at a minimum of every hour; some as frequently as every 5 seconds.
A.12.4.1 Event logging	Included	Business requirements related to IP
A.12.4.2 Protection of log information	Included	6-month log retention allows for complete incident response.
A.12.4.3 Administrator and operator logs	Included	Admins do have rights over local logs, so an independent log would be needed.
A.12.4.4 Clock synchronisation	Included	Servers use NTP System/ Keysight Primary Time Server

A.12.5.1 Installation of software on operational systems	Included	Software installation occurs on servers and workstations.
A.12.6.1 Management of technical vulnerabilities	Included	Large number of owned servers and workstations requires vulnerability management.
A.12.6.2 Restrictions on software installation	Included	About 100 workstations could be at risk.
A.12.7.1 Information systems audit controls	Included	Internal Technical Audits are part of the Keysight ISMS.
A.13.1.1 Network controls	Included	Remote offices use VPN and there is a Keysight Intranet.
A.13.1.2 Security of network services	Included	Servers are in the Agilent data center, but Keysight staff manage and contribute to network security.
A.13.1.3 Segregation in networks	Included	Keysight manages multiple domains with different levels of protection.
A.13.2.1 Information transfer policies and procedures	Included	All network traffic is encrypted.
A.13.2.2 Agreements on information transfer	Included	The only way for external parties to transfer information is through VPN control or, for email, using Microsoft 365 with SSO.
A.13.2.3 Electronic messaging	Included	Email is through Office 365 apps or webmail, and messaging is Cisco Jabber, both of which use SSO.
A.13.2.4 Confidentiality or non-disclosure agreements	Included	All employees and contractors sign confidentiality agreements.
A.14.1.1 Information security requirements analysis and specification	Included	Systems in scope include enterprise software, servers, and workstations. Keysight has no specific IS requirements for hardware procurement.
A.14.1.2 Securing application services on public networks	Included	All application services on public networks are by large, trusted cloud providers (Microsoft 365 for email and SAP Success Factors for HR)
A.14.1.3 Protecting application services transactions	Included	All traffic is https encrypted, including intranet services.
A.14.2.1 Secure development policy	**Excluded**	Software development is out of scope
A.14.2.2 System change control procedures	**Excluded**	All development, including version modifications, is out of scope. See A.14.2.1.
A.14.2.3 Technical review of applications after operating platform changes	Included	There are business critical applications running on the Linux servers which do need occasional update.
A.14.2.4 Restrictions on changes to software packages	**Excluded**	Software development is out of scope
A.14.2.5 Secure system engineering principles	Included	Although Keysight software is excluded from scope, and all business applications are off-the-shelf, some engineering is performed for the network, and firewalls are part of the integrated design.
A.14.2.6 Secure development environment	**Excluded**	Software development is out of scope
A.14.2.7 Outsourced development	**Excluded**	Software development is out of scope
A.14.2.8 System security testing	**Excluded**	Software development is out of scope

A.14.2.9 System acceptance testing	Included	Although software development testing is out of scope, there are enterprise software purchases which fall under this control.
A.14.3.1 Protection of test data	**Excluded**	Software development is out of scope
A.15.1.1 Information security policy for supplier relationships	Included	Keysight uses information services vendors from time to time.
A.15.1.2 Addressing security within supplier agreements	Included	Keysight has identified SaaS security (which includes acceptable use provisions), personal data protection, and confidentiality as major supplier requirements.
A.15.1.3 Information and communication technology supply chain	Included	Only commercially available off-the-shelf vendor products (no critical components) are purchased. There are no managed supply chain equipment or software components.
A.15.2.1 Monitoring and review of supplier services	Included	There is currently one supplier providing services under scope, Deloitte, who performs incident management and threat hunting.
A.15.2.2 Managing changes to supplier services	Included	There is currently one supplier providing services under scope, Deloitte, who performs incident management and threat hunting.
A.16.1.1 Responsibilities and procedures	Included	Security Events and Incidents are managed and appropriately addressed.
A.16.1.2 Reporting information security events	Included	Security Events and Incidents are managed and appropriately addressed.
A.16.1.3 Reporting information security weaknesses	Included	All staff and contractors are required to report weaknesses in the Keysight system.
A.16.1.4 Assessment of and decision on information security events	Included	Security Events and Incidents are managed and appropriately addressed.
A.16.1.5 Response to information security incidents	Included	Security Events and Incidents are managed and appropriately addressed.
A.16.1.6 Learning from information security incidents	Included	Incidents are reviewed for actionable lessons learned.
A.16.1.7 Collection of evidence	Included	No incidents have resulted in legal action yet, but the possibility exists.
A.17.1.1 Planning information security continuity	Included	Continuity under scope is data recovery from the backup data center after an event.
A.17.1.2 Implementing information security continuity	Included	Continuity under scope is data recovery from the backup data center after an event.
A.17.1.3 Verify, review and evaluate information security continuity	Included	Continuity/ DR is regularly tested.
A.17.2.1 Availability of information processing facilities	Included	The Colorado Springs Data Center has a redundant backup in Dallas. Critical systems are backed up at a minimum of every hour; some as frequently as every 5 seconds.
A.18.1.1 Identification of applicable legislation and contractual requirements	Included	Only current requirement is NIST 800-171 due to DoD work; NIST requirements are referenced on each policy, and policies were built from NIST.

A.18.1.2 Intellectual property rights	Included	Others' IP is controlled via the Acceptable Use Policy; license management is controlled directly by the vendor.
A.18.1.3 Protection of records	Included	All Information Security - relevant records are kept on SharePoint except event logs which are stored in the SIEM for 3 months.
A.18.1.4 Privacy and protection of personally identifiable information	Included	The only personally identifiable information stored by Keysight is HR data which is in the SAP SuccessFactors cloud. SAP represents that the SuccessFactors system controls are equivalent to ISO 27001.
A.18.1.5 Regulation of cryptographic controls	Included	Keysight is subject to NIST 800-171 cryptographic requirements due to work for the DoD.
A.18.2.1 Independent review of information security	Included	Keysight Internal Audit performs targeted IS audits throughout the year to address changes and vulnerabilities, separate from the formal ISO Internal Audit.
A.18.2.2 Compliance with security policies and standards	Included	Keysight managers are responsible for verifying their compliance with relevant policies.
A.18.2.3 Technical compliance review	Included	Keysight performs Penetration Tests and other technical compliance reviews.