Keysight's Borderless Information Security Program

Keysight Technologies information security program applies a risk-based approach that has foundations in industry standards and best practices. Our information security operations and procedures provide a comprehensive Information Security Management System (ISMS) in order to maintain the confidentiality, integrity, and availability of information and systems in our environment. Information security is an important priority and we continuously invest in our People, Processes, and Tools to strengthen our security posture to protect both Keysight's data and our Customer's data.

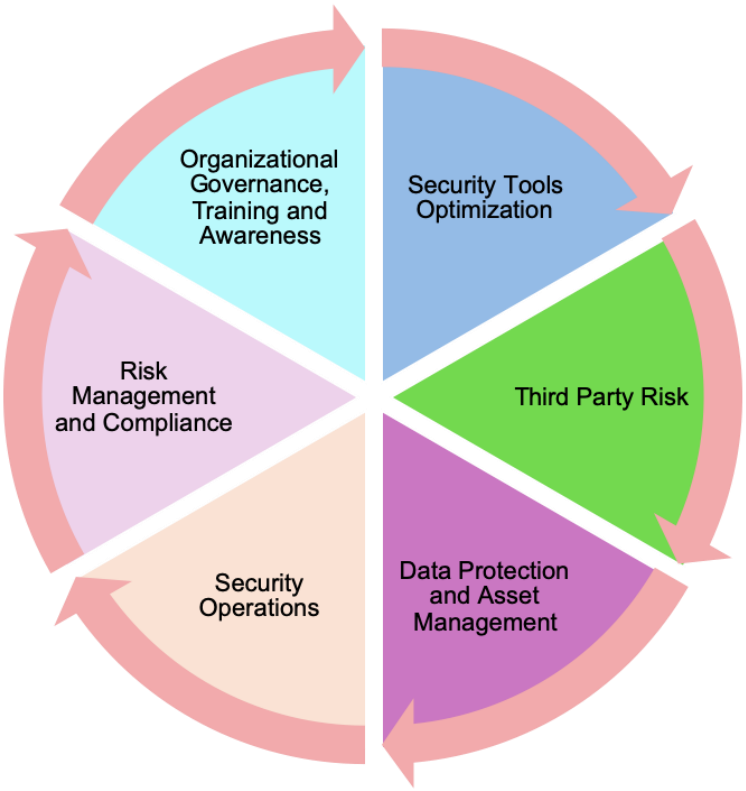
Keysight is ISO27001, UK Cyber Essential Plus, and PCI-DSS certified. Keysight Information Security Policies are based on NIST SP 800-171 and apply enterprise-wide.

Keysight has a borderless, enterprise-wide approach to information security and has a dedicated Information Security and Compliance organization (ISC) that owns and operates the information security management system. The ISC organization reports directly to Keysight's Chief Information Security Officer (CISO) and includes functions such as:

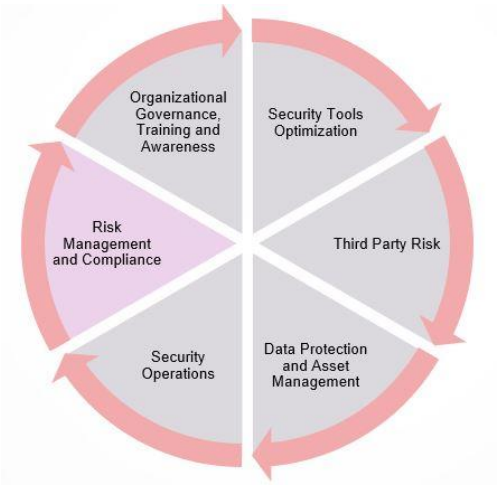
1) Information Security Policy Management
2) Risk Management
3) Vulnerability Management
4) Compliance Assurance
5) Identity and Access Management
6) Incident Management
7) Security Awareness and Education
8) IT Disaster Recovery

KEYSIGHT TECHNOLOGIES

Keysight's **Borderless Information Security Program** focuses on the following:



Risk Management and Compliance



Keysight uses robust programs and processes to make informed decisions about remediating, mitigating, or accepting risks to assist the organization in securely achieving its objectives. Keysight adheres to mandated laws and regulations, customer compliance requirements, and our organizations' policies, procedures, and processes.

Risk Management – Keysight's risk management program is used to assess, document, monitor, and report risk. Risk exposure, avoidance, mitigation, and acceptance are analyzed, documented, and reviewed.

Information Security Review – The ISR process assesses the risk to Keysight systems and information by analyzing the likelihood and impact of harmful events. It delivers recommendations for reducing the risk involved in activities and processes so that they can be executed more safely and confidently.

Compliance Assurance – Keysight has operations worldwide and is subject to a variety of regulatory requirements, including SOX, DFARS, GDPR, HIPAA, and PCI-DSS, ensuring that we implement a strategic plan to ensure compliance.

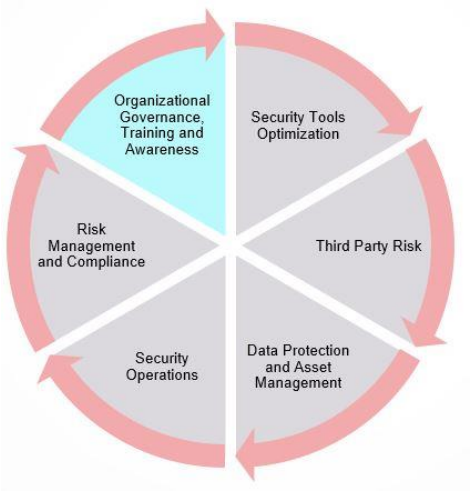
Independent Assessments – Approved third party companies are used for ensuring regulatory compliance, control performance validation, penetration testing, and impartial risk assessments.

Vulnerability Management – The vulnerability management team has visibility to current trends and events within the information security community. This visibility is used to proactively protect our environment.

Customer Compliance – Keysight receives and responds to our customer's security and compliance inquiries. Where applicable this input is taken into consideration for policies or controls.

Organizational Governance, Training and Awareness

Organizational governance activities ensure that critical management information reaching the stakeholders is complete, accurate and timely to enable appropriate management decision making, and provide the control mechanisms to ensure that strategies, directions and instructions from management are carried out systematically and effectively.



Information Security and Compliance – Organizational meetings are held to discuss and inform management, stakeholders, and employees of strategies and direction. These meeting include areas from all functions in the organization to provide alignment and awareness.

Performance Metrics – Metrics on the performance, availability, and health of Keysight's IT environment are formally reviewed every month by top management and representatives from all operational areas of IT and other stakeholders.

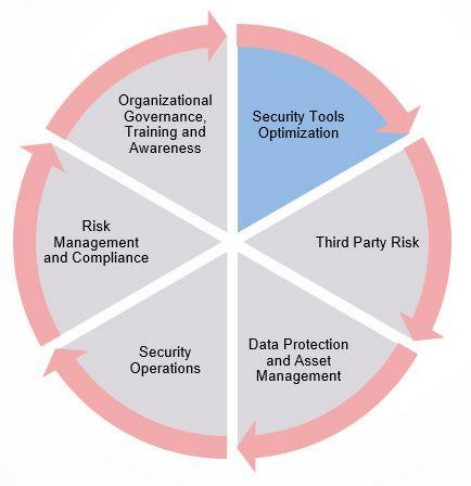
Change Management Process – Controls are in place to ensure that changes in production environments are deployed in a controlled fashion, and are documented, tested, and approved prior to deployment.

Security Awareness and Education – Continuous training programs are required to be completed by employees worldwide. These programs cover security, Standards of Business Conduct, and compliance. Additionally, there are enterprise-wide phishing simulation tests and function/role-based trainings as required.

Training – Keysight encourages and supports employee's continual development and education through investing in external trainings and certifications relevant to their scope of work.

Information Security Policy Management – Keysight has structured Information Security Policies that are reviewed at least annually and updated as needed. The policies are based off NIST SP 800-171.

Security Tools Optimization



Security tools are critical for Keysight to predict, protect, and respond to potential risks and threats to the data and systems in our environment. Advanced persistent threats and zero-day vulnerabilities require constant monitoring by automated technologies combined with human oversight.

Network – Keysight uses firewalls, intrusion detection systems, intrusion prevention systems, and web content filtering protections for traffic traversing ingress/egress points with non-Keysight networks. Internet facing systems are placed in a DMZ and the applications are further protected behind a web application firewall. Additionally, Keysight uses 802.1x to validate devices that are trying to connect to Keysight's network.

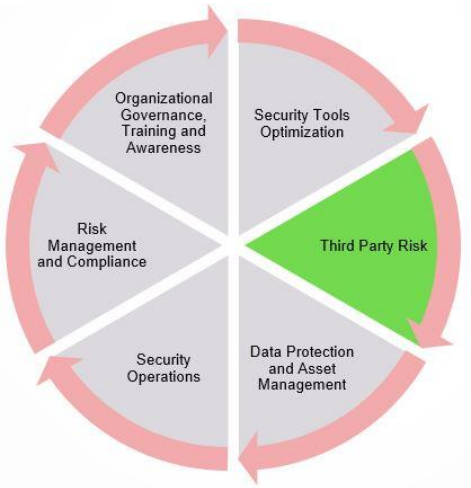
Systems – Up to date antivirus and malware detection tools are installed on all endpoints. Scans are configured to be performed on access as well as full system scans. Full disk encryption is used as appropriate. System hardening is performed by restricting administrative rights, disabling unneeded and potentially insecure services, removing default passwords, and applying Keysight's security configuration.

Security Information and Event Management – Keysight utilizes a SIEM to process logs and events. The SIEM correlates input from across the Keysight network and creates alerts when suspicious behavior is detected.

Email Protections – Phishing remains one of the more popular ways that bad actors try to gain access into network. Keysight has deployed tools and services for enhanced email security to protect against phishing attacks and to reduce spam, bulk, and other unwanted emails.

Privileged Account Management - Keysight has PAM tools that enable the securing, control, managing, and monitoring of privileged access to its critical assets.

Third Party Risk



Third party partners with access to the Keysight's network and information or that supply Keysight with managed services present additional risk that needs to be evaluated and controlled. Keysight has processes and procedures in place to constantly review and evaluate third party risk.

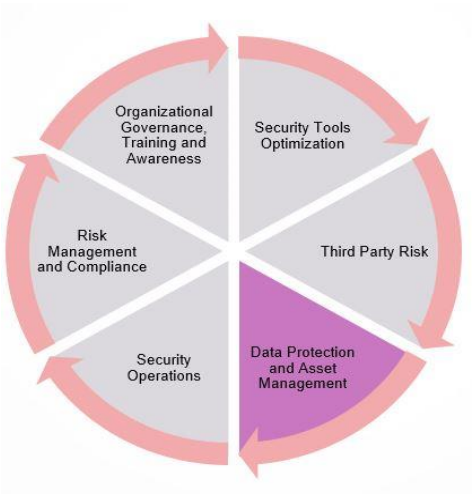
Supply Chain Risk Management – Keysight monitors its suppliers' information security via the supply chain risk management program which includes supplier audits and independent monitoring of suppliers' information security posture.

Third Party Access – Third party access to Keysight's networks is catalogued and reviewed. Third parties are only granted access to the information or systems that they need in order to carry out their work.

Supplier Audits – Keysight's Internal Audit organization performs independent audits to help to identify potential control weaknesses, compliance concerns or operational inefficiencies in suppliers' operation and Keysight IT's oversight and governance processes.

Data Protection and Asset Management

In order to protect Keysight's data and assets, Keysight keeps an up-to-date inventory of assets and employs many layers of controls to ensure the confidentiality, integrity, and availability of its information.



Identity and Access Management –Identities are securely managed with robust account provisioning and deprovisioning processes. Access controls include multi-factor authentication, the application of the principle of least privilege, and periodic privileged account reviews. Third parties are vetted, and their access is periodically reviewed.

Mobile Device Management – All mobile devices on the Keysight network that access Keysight systems or information have their configurations controlled and use encryption.

Encryption – Encryption is used where required and includes information in motion and at rest.

Database Activity Monitoring – A database activity monitoring tool is used to independently monitor and audit database activity. This ensures that Keysight can identify and report fraudulent or other undesirable database activity.

Asset Management – Inventory of assets are kept in our enterprise databases. This inventory includes details of the asset including the configuration, software installed and running, and the owner.

Media Disposal – Keysight uses advanced techniques for data destruction and has policies that require all media to be sanitized before it is disposed of, re-purposed, or when no longer in use.

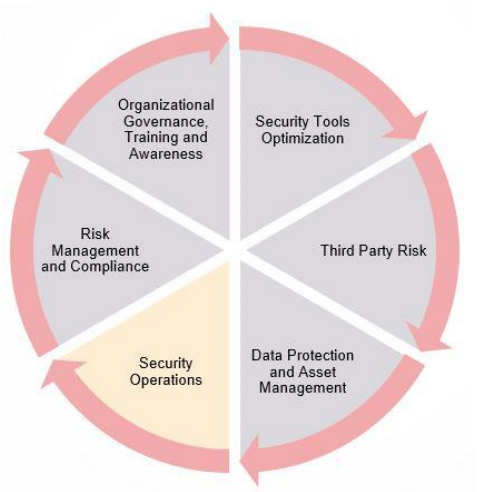
IT Disaster Recovery – Disaster recovery plans and processes are documented and regularly tested. The disaster recovery site is geographically separated from the enterprise data center.

Backup – Backups are in place and configured with a backup frequency that is applicable to the information being backed up. Keysight tests backups on a periodic basis to ensure they can be correctly restored.

Physical Security – Keysight's facilities are protected with security officers, badge access controls, and video monitoring. Data centers are protected by security officers, IT professionals, video cameras, environmental monitoring, and redundant utility connections.

Security Operations

Keysight has processes in place for detection, prompt action, and responses to potential attacks, breaches, or disruptions to reduce the impact on the confidentiality, integrity, and availability of the environment. Keysight focuses on the people and process that allow us to respond appropriately.



Security Operations Center – Keysight operates an in-house dedicated 24x7 Security Operations Center with human and machine monitoring for potential IT security events.

IT operations – Keysight has IT support operations teams which monitor the health of the IT environment 24x7. This includes real-time network monitoring.

Event Correlation - A SIEM (Security Information and Event Management) is used for monitoring and performing correlations across the entire Keysight network to identify, report, and alert on security events and anomalies.

Incident Response Team – This dedicated team leads the investigation into security related events. The security related events come from many different sources including the SOC (Security Operations Center), IT Operations, Employees, Management, and Customers.

Incident Response Plan – Keysight has a documented security incident response plan that defines roles and responsibilities. This plan includes processes and procedure for responding to incidents, including the necessary communication channels and sequences.

Incident Management – Keysight has IT support teams to address non-security related incidents and events, to ensure a robust environment, and to maintain availability and integrity of the systems and data.

Communications – Processes are in place to notify impacted stakeholders during and after a reportable event.

Additional Resources

- ISO 27001 Certificate

For additional questions, please contact Keysight

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus