COMPLIANCE ASSESSMENT REPORT

NIST SP 800-171

STREAMLINE CIRCUITS

1401 MARTIN AVENUE
SANTACLARE, CA

DATES: 21-DEC-2017 TO 23-DEC-2017
BR#: 10010858

1. Assessment recommendation

Thank you for your trustful cooperation during our recent assessment of your organization. This report details the assessment results including strengths, opportunities, and weaknesses. These results were presented to your management at the closing meeting of the assessment. You can use these results to improve the effectiveness of your information security posture. We look forward to continuing our partnership towards sustainable business success.

Current scope of assessment:	Protection of Controlled Unclassified Information (CUI) stored in the organization's information systems.
Number of personnel included in the scope	10

In reference to NIST SP 800-171, the assessment team recommends to DQS:

☒ Issuance of the letter of compliance (LOC)

☐ Issuance of the letter of compliance (LOC) as soon as implementation of corrective actions has been demonstrated

Please remember to notify DQS about any significant change to your security management system at your earliest convenience. Together we will then coordinate appropriate measures to maintain your current LOC.

All assessment findings are based on a sampling process, targeted towards reliable evidence for effective implementation and compliance of the security controls. Where applicable findings and required corrective action plans were or will be agreed upon with the responsible managers, steps have been or will be defined to resolve such non-conformity. Further business aspects may exist, positive or negative, which have not been reviewed by the assessment team. It is the organization ´s responsibility to investigate and evaluate the potential impact and scope of findings, thus continuously ensuring full compliance to the applied standard(s).

2. Executive summary

Streamline Circuit is a manufacturer of printed circuit boards. Government customers / Defense contractors provides drawing/specifications for printed circuit boards. Those are considered as Controlled Unclassified Information (CUI). Defense Acquisition Federal Regulation Supplement (DAFRS) requires all government contractors handling CUI to comply with the requirements of NIST SP 800-171 before December 31, 2017.

Sufficient evidence of compliance observed against the additional requirements of the NIST 800-171 during this assessment. For sustaining compliance to these requirements, Streamline Circuit may like to consider ISO IEC 27001 certification.

Details statement of compliance against each controls are provided in the next section.

3.3. Assessment results

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.1.1	Basic	Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Access control policy is defined in the IT Policies and procedure document, Pages (6-8)	S
3.1.2	Derived	Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Access levels are defined by department and job functions. User access is authenticated by the Active Directory.	S
3.1.3	Derived	Access Control	Control the flow of CUI in accordance with approved authorizations.	Process workflow diagram shows flow of CUIs. Different access levels for different groups (e.g. Sales, Engineering and Production) and controlled through Active Directory.	S
3.1.4	Derived	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Separation of duties implemented in handling CUIs. In the production process, each stage gets access to part of the design element that section is responsible for (e.g. drilling diagram of the PCB)	S
3.1.5	Derived	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Role based access control is based on the principle of leas privilege. Only Engineering team have full access to unencrypted CUI data stored in the Genesis application.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.1.6	Derived	Access Control	Use non-privileged accounts or roles when accessing non security functions.	IT has one admin and one non-admin account.	S
3.1.7	Derived	Access Control	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Regular users do not have admin rights to execute privileged functions. Controlled through PCMatic. System log files are audited daily.	S
3.1.8	Derived	Access Control	Limit unsuccessful logon attempts.	Defined as 5 attempts in 30 minutes in the Active Directory.	S
3.1.9	Derived	Access Control	Provide privacy and security notices consistent with applicable CUI rules.	Privacy and acceptable use policy is acknowledged by all employees at the time of hiring.	S
3.1.10	Basic	Access Control	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Automatic screen lock enabled after 5 minutes.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.1.11	Derived	Access Control	Terminate (automatically) a user session after a defined condition.	Idle VPN session automatically terminated after 1 hour.	S
3.1.12	Derived	Access Control	Monitor and control remote access sessions.	VPN activity log monitored.	S
3.1.13	Derived	Access Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Microsoft VPN is used for remote access.	S
3.1.14	Derived	Access Control	Route remote access via managed access control points.	VPN connections are authenticated through Active Directory.	S
3.1.15	Derived	Access Control	Authorize remote execution of privileged commands and remote access to security-relevant information.	Same as above	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.1.16	Derived	Access Control	Authorize wireless access prior to allowing such connections.	Wireless access is only for email and internet. Users must be authenticated through AD before accessing CUIs.	S
3.1.17	Derived	Access Control	Protect wireless access using authentication and encryption.	Wireless access is protected using WEP encryption.	S
3.1.18	Derived	Access Control	Control connection of mobile devices.	Connection of mobile devices requires management approval. Connections controlled by IT. CUIs cannot be accessed from mobile devices.	S
3.1.19	Derived	Access Control	Encrypt CUI on mobile devices.	CUIs are sent or received as encrypted attachments with email. Mobile devices do not ability to decrypt the attachments.	S
3.1.20	Derived	Access Control	Verify and control/limit connections to and use of external information systems.	Do not connect to any external information systems.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.1.21	Derived	Access Control	Limit use of organizational portable storage devices on external information systems.	USB ports are disabled on all machines.	S
3.1.22	Derived	Access Control	Control information posted or processed on publicly accessible information systems.	Data classification policy defines publicly accessible information's. No data transactions are done using publicly accessible system (i.e. corporate website)	S
3.2.1	Basic	Awareness and Training	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	New employee orientation and training process.	S
3.2.2	Basic	Awareness and Training	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	New employee orientation and training process.	S
3.2.3	Derived	Awareness and Training	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Orientation training records verified. Subjects includes OPSEC security, ITAR, Right to know policy etc.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.3.1	Basic	Audit and Accountability	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	System log files audited daily using automated and manual way.	S
3.3.2	Basic	Audit and Accountability	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Same as above	S
3.3.3	Derived	Audit and Accountability	Review and update audited events.	Daily review of backup log, looks for failed backups.	S
3.3.4	Derived	Audit and Accountability	Alert in the event of an audit process failure.	ObserVium tool monitors servers and network devices. Alerts set up for various events in the tool.	S
3.3.5	Derived	Audit and Accountability	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	Same as above	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.3.6	Derived	Audit and Accountability	Provide audit reduction and report generation to support on-demand analysis and reporting.	Same as above	S
3.3.7	Derived	Audit and Accountability	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Server time is synchronized with Microsoft time service	S
3.3.8	Derived	Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.	Log files are protected and retained following IT Policies and Procedure.	S
3.3.9	Derived	Audit and Accountability	Limit management of audit functionality to a subset of privileged users.	Only system admin can use ObserVium	S
3.4.1	Basic	Configuration Management	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Inventory of hardware and software assets maintained.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.4.2	Basic	Configuration Management	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Asset inventory is protected through access control policy and change control process.	S
3.4.3	Derived	Configuration Management	Track, review, approve/disapprove, and audit changes to information systems.	Change management system controls changes to Systems and infrastructures.	S
3.4.4	Derived	Configuration Management	Analyze the security impact of changes prior to implementation.	Impact meetings conducted every week to analyze impacts of changes.	S
3.4.5	Derived	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Access control policy and Change control process	S
3.4.6	Derived	Configuration Management	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	Principle of leas privilege implemented using Access Control policy.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.4.7	Derived	Configuration Management	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Implemented using PCMatic whitelisting feature.	S
3.4.8	Derived	Configuration Management	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	White list software policy implemented using PCMatic	S
3.4.9	Derived	Configuration Management	Control and monitor user-installed software.	Same as above	S
3.5.1	Basic	Identification and Authentication	Identify information system users, processes acting on behalf of users, or devices.	Active Directory is used for authentication	S
3.5.2	Basic	Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	same as above	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.5.3	Derived	Identification and Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Separate login credential required to access Genesis or other applications.	S
3.5.4	Derived	Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Policy prevents storing of passwords in web browsers.	S
3.5.5	Derived	Identification and Authentication	Prevent reuse of identifiers for a defined period.	Active Directory remembers 5 previous passwords	S
3.5.6	Derived	Identification and Authentication	Disable identifiers after a defined period of inactivity.	Idle Active Directory accounts disabled after 90 days.	S
3.5.7	Derived	Identification and Authentication	Enforce a minimum password complexity and change of characters when new passwords are created.	Password complexity implemented using Active Directory.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.5.8	Derived	Identification and Authentication	Prohibit password reuse for a specified number of generations.	Active Directory remembers 5 previous passwords	S
3.5.9	Derived	Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.	Temporary passwords are changed after first log in.	S
3.5.10	Derived	Identification and Authentication	Store and transmit only encrypted representation of passwords.	Password never sent via email	S
3.5.11	Derived	Identification and Authentication	Obscure feedback of authentication information.	Password entry is masked	S
3.6.1	Basic	Incident Response	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	Security incident response policy defined and implemented.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.6.2	Basic	Incident Response	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	Incident response process addresses recording, investigation, communications and resolution of incidents.	S
3.6.3	Derived	Incident Response	Test the organizational incident response capability.	DR plan and backups are tested periodically.	S
3.7.1	Basic	Maintenance	Perform maintenance on organizational information systems.	PCMatic is setup to run maintenance on a daily basis of all machines. This maintenance includes patches, malware detection, registry errors, health scans etc. All records are sent to the incident reporting system.	S
3.7.2	Basic	Maintenance	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Same as above	S
3.7.3	Derived	Maintenance	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Equipment are not sent off site for repair.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.7.4	Derived	Maintenance	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	Anti-virus control implemented using PCMatic	S
3.7.5	Derived	Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Secondary authentication required to access Genesis which contains CUIs	S
3.7.6	Derived	Maintenance	Supervise the maintenance activities of maintenance personnel without required access authorization.	Maintenance engineers are escorted and their work supervised.	S
3.8.1	Basic	Media Protection	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Use of all types of removable media prohibited within the company. All USB ports are disabled.	S
3.8.2	Basic	Media Protection	Limit access to CUI on information system media to authorized users.	Same as above	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.8.3	Basic	Media Protection	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	Hard disks are destroyed before recycling machines	S
3.8.4	Derived	Media Protection	Mark media with necessary CUI markings and distribution limitations.	No media used	S
3.8.5	Derived	Media Protection	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Same as above	S
3.8.6	Derived	Media Protection	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Same as above	S
3.8.7	Derived	Media Protection	Control the use of removable media on information system components.	Same as above	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.8.8	Derived	Media Protection	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Same as above	S
3.8.9	Derived	Media Protection	Protect the confidentiality of backup CUI at storage locations.	CUI backup are stored in another secured server.	S
3.9.1	Basic	Personnel Security	Screen individuals prior to authorizing access to information systems containing CUI.	All full time employee goes through background screening per California law.	S
3.9.2	Basic	Personnel Security	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Physical and logical access are disabled when employees leaves. USB ports are disabled on all machines.	S
3.10.1	Basic	Physical Protection	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Role based access policy implemented. Server room access is restricted to only IT personnel. Only Engineering team can access Genesis software.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.10.2	Basic	Physical Protection	Protect and monitor the physical facility and support infrastructure for those information systems.	Proximity card reader is installed on all building doors. Visitors can only access through the main lobby. Visitor badge is issued. Video camera is installed in Key positions to monitor facility.	S
3.10.3	Derived	Physical Protection	Escort visitors and monitor visitor activity.	General visitors are escorted all times. Only ITAR authorized visitors gets "No escort required" badges. Facility is always under video surveillance.	S
3.10.4	Derived	Physical Protection	Maintain audit logs of physical access.	Badge access system maintains access log. System also has capability to generate reports on the log activities.	S
3.10.5	Derived	Physical Protection	Control and manage physical access devices.	Physical cards are issued to new hires following access authorization process. Access are terminated in the system when employee leaves.	S
3.10.6	Derived	Physical Protection	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	There is no alternate work site. CUIs cannot be accessed remotely.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.11.1	Basic	Risk Assessment	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	Risk assessment policy defined. Infrastructure is scanned bi-annually.	S
3.11.2	Derived	Risk Assessment	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	Vulnerability scanning done twice a year.	S
3.11.3	Derived	Risk Assessment	Remediate vulnerabilities in accordance with assessments of risk.	Remediation actions are prioritized based on the severity.	S
3.12.1	Basic	Security Assessment	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	Security controls per NIST SP 800-171 have been defined and implemented. Evidence of internal review and review by external consultants available.	S
3.12.2	Basic	Security Assessment	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	Action plan developed to correct deficiencies identified after such reviews.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.12.3	Basic	Security Assessment	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Annual assessment will be conducted by DQS. The organization is also planning to implement ISO 27001 and merge NIST 800-171 controls with ISO 27001 system.	S
3.13.1	Basic	System and Communications Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	ObserVium tool monitors Network infrastructure including Firewall events.	S
3.13.2	Basic	System and Communications Protection	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	IT remote access policy defined	S
3.13.3	Derived	System and Communications Protection	Separate user functionality from information system management functionality.	Regular users privilege and System administrator privilege defined in the AD.	S
3.13.4	Derived	System and Communications Protection	Prevent unauthorized and unintended information transfer via shared system resources.	Prevented using role based access control and segregation of duties. System log files keeps audit trails of system usage.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.13.5	Derived	System and Communications Protection	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Only publicly accessible system is company website. It is on a completely separate network from the internal systems that stores CUIs.	S
3.13.6	Derived	System and Communications Protection	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Firewall allows network traffic as defined in the policy.	S
3.13.7	Derived	System and Communications Protection	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	Only remote access allowed using VPN authenticated through Active Directory.	S
3.13.8	Derived	System and Communications Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	CUI transmission is always encrypted or downloaded from customer's portal through secured connection.	S
3.13.9	Derived	System and Communications Protection	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Idle VPN sessions automatically terminated after 60 minutes.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.13.10	Derived	System and Communications Protection	Establish and manage cryptographic keys for cryptography employed in the information system;	Encryption keys are created by customer ad provided in a secured manner. Keys are destroyed after use.	S
3.13.11	Derived	System and Communications Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Determined by customers	S
3.13.12	Derived	System and Communications Protection	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Such computing are prohibited.	S
3.13.13	Derived	System and Communications Protection	Control and monitor the use of mobile code.	Controlled using the whitelisting through PCMatic.	S
3.13.14	Derived	System and Communications Protection	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	VOIP network is separated from LAN	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.13.15	Derived	System and Communications Protection	Protect the authenticity of communications sessions.	Done through Microsoft VPN	S
3.13.16	Derived	System and Communications Protection	Protect the confidentiality of CUI at rest.	CUI are stored as encrypted files in the server and deleted following ITAR regulations after use.	S
3.14.1	Basic	System and Information Integrity	Identify, report, and correct information and information system flaws in a timely manner.	Alerts and warnings are generated using ObserVium	S
3.14.2	Basic	System and Information Integrity	Provide protection from malicious code at appropriate locations within organizational information systems.	PCMatic used for protection	S
3.14.3	Basic	System and Information Integrity	Monitor information system security alerts and advisories and take appropriate actions in response.	Alerts generated from the monitoring tool are sent to the ticketing system.	S

Control Number	Control Type	Control Family	Control Text	Observation	Status
3.14.4	Derived	System and Information Integrity	Update malicious code protection mechanisms when new releases are available.	PCMatic used for protection	S
3.14.5	Derived	System and Information Integrity	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Same as above	S
3.14.6	Derived	System and Information Integrity	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Same as above	S
3.14.7	Derived	System and Information Integrity	Identify unauthorized use of the information system.	System log files audited daily using automated and manual way.	S

Report prepared on: 29-Dec-17 Prepared by: Subrata Guha

Technical review completed on: <Date> Technical reviewer: <Name>