Standard Operating Procedure

SOP 1055-01

Title: Computer System Controls			
Effective Date:	October 1, 2006	Previous Version:	None
Reason for Update:	New SOP		

Owner: Chief Technology Officer Signature/ Date	Location Portland

Objective The objective of this Standard Operating Procedure (SOP) is to provide an overview of the identification and protection of proprietary information.

Scope This document establishes the procedures used to identify and label proprietary information and protect it from inadvertent or unauthorized disclosure, modification or destruction.

Applicable To All SDLC Security Administration Staff

Sections
Section 1: Procedure Diagram
Section 2: Roles and Responsibilities
Section 3: Metrics
Section 4: Procedure Activities
Section 5: Forms
Section 6: Exemptions
Section 7: Tools/Software/Technology Used

Attachments None

Related Procedures
SOP 1005: Release Planning
SOP 1050: Electronic Information Security Standards
SOP 1051: Security Administration
SOP 1053: Appropriate Use of Computer Resources
SOP 1054: Non-SDLC Use of SDLC Computers
SOP 1055: Computer Systems Controls

Definitions

Computer systems controls are an integral part of SDLC's internal control structure and are organized into two categories: General Computer System Controls and Application System Controls. Application systems are composed of programs written for or by the user to support the user's business functions. The responsibility for implementing and enforcing data processing controls resides with the system owners, users, and data processing equipment custodians. These standards apply universally to all SDLC computing environments, which include personal computers, workstations, computer centers, and local area, facility and wide area networks

In management's selection of procedures and techniques of control, the degree of control implemented is a matter of reasonable business judgment. The common guideline that should be used in determining the degree of internal controls implementation is that the cost of a control should not exceed the benefit derived.

SECTION 1: PROCEDURE DIAGRAM

- None at this time

SECTION 2: ROLES AND RESPONSIBILITIES

Role	Responsibility
Managers and Directors	Implement and enforce this policy and procedure within their respective business entities.
Employees	Each employee has a responsibility to implement this policy for all systems to which he/she has been assigned ownership.
Auditors	Monitor compliance with this procedure and determine that suitable tools and training are available in audited departments.

SECTION 3: METRICS

- None at this time

SECTION 4: PROCEDURE ACTIVITIES

The following schedule provides information with respect to the treatment to be given to SDLC systems. It is organized by type of classification. Within each classification the type of action and the procedures that must accompany that specific action then organizes it.

System Owners and Custodians of Equipment

	Standard of Control		Risk if Standard is Not Achieved
4.1	Corporate/Sector/Group Controllers are responsible for ensuring an owner is assigned for each application system including manufacturing and engineering systems. System owners are the primary system users. For a system shared among multiple departments or business groups, the system owner is defined as the user or group of users with the primary responsibility for updating the application files. *Refer to risk A-1*	A.1	Systems may not be properly maintained and controlled without system owner sponsorship.
4.2	Corporate/Sector/Group general or department managers, in coordination with Information Systems management, must maintain up-to-date lists of system owners. *Refer to risks: A-3, A-4*	A.2	Changes and access to systems may not be properly authorized.
4.3	The system owner must approve system requirements/design or system changes, assign security classifications, authorize access to system data files, and acknowledge acceptance of new systems and system changes. *Refer to risk: A-2*	A.3	MIS personnel may seek approval for system changes from someone other than the system owner

	Standard of Control		Risk if Standard is Not Achieved
4.4	Corporate/Sector/Group general or department managers are responsible for ensuring a custodian is assigned for all data processing equipment including computer centers, remote processing sites, local area networks, engineering workstations, departmental and personal computers, and data storage sites. *Refer to risk: A-5*	A.4	Management personnel may change responsibilities without transferring system ownership.
4.5	Custodians of data processing equipment and application data must: a) Provide a physical environment with safeguards against unauthorized removal or destruction of data or data processing equipment; b) Arrange for the backup and retention of critical application data files and programs in secure locations outside the facility where normal processing occurs; c) Arrange for equipment and/or alternate computing facilities sufficient to meet established disaster recovery priorities; d) Provide sufficient computer resources to respond to the data processing needs of the users who operate systems at their facility, department or local area network; and e) Ensure procedures exist to comply with agreements for use of licensed software. *Refer to risks: A-6, A-7, A-8, A-9, A-10*	A.5	The responsibilities associated with operating and/or maintaining data processing facilities may not be clearly defined.

	Standard of Control		Risk if Standard is Not Achieved
4.6	Corporate/Sector/Group organizations responsible for software development or maintenance are responsible for preparing and maintaining detailed data processing policies and procedures. The policies and procedures must include: a) Criteria for management approval of system changes to move software from a test to production status; b) Documentation standards for system architecture, logical design, and physical design; and c) Software coding standards, which define program structure, guidelines for logic complexity, and data element naming conventions. *Refer to risk: A-10*	A.6	Computer equipment may be damaged by fire or other natural causes or intentionally damaged by unauthorized persons
		A.7	Backup files may not be available for processing in the event of a disaster.
		A.8	SDLC's ability to conduct business may be significantly impaired in the event of a disaster at a computer or network site.
		A.9	Adequate computer resources may not be available to meet business requirements and growth.
		A.10	SDLC may be liable for misuse or unauthorized copying of proprietary software.
		A.11	The responsibilities associated with operating and/or maintaining system software operations and application documentation may not be clearly defined.

General Data Processing Controls

General data processing controls are primarily concerned with the operation and protection of computer resources, and the development and integrity of application systems and data. General data processing controls are the joint responsibility of user and data processing equipment custodians. The adequacy of general data processing controls within an organization provides the basis for the level of reliance placed upon application controls and, in turn, business and accounting controls for the accuracy and integrity of business and financial information.

	Standard of Control		Risk if Standard is Not Achieved
4.7	Management may designate certain computing areas as requiring restricted access. Access to restricted computing areas must be limited to authorized individuals. Examples of restricted areas are product design departments, computer centers and network file server locations. The following control techniques must be employed for these areas: a) Physical access to computer and network hardware, software, data, and documentation must be specifically authorized by management and restricted to only those personnel requiring such access for performance of assigned functional responsibilities; *Refer to risks: B-1, B-2* b) All entrances/exits to restricted computing areas must be physically secured; *Refer to risks: B-1, B-2, B-3*	B.1	Computer hardware, software, data, and documentation may not be adequately protected from damage or theft.

	Standard of Control		Risk if Standard is Not Achieved
	c) All keys, keycards, badges, etc., used to limit access to restricted computing areas must be confiscated by management upon employee termination or transfer. All combinations or passwords to restrictive areas and support areas must be changed periodically and upon employee termination or transfer; *Refer to risks: B-1, B-2, B-3* d) All physical access to computer hardware, software, data, and documentation by suppliers and visitors must be specifically authorized by management. All suppliers and visitors must be accompanied by authorized personnel; and *Refer to risks: B-1, B-2* e) All removal of computer equipment and data files containing proprietary information must be specifically authorized by management, recorded, and reconciled. All data files removed must be handled in accordance with their security classification. *Refer to risks: B-1, B-2*		
4.8	Physical computer sites must be prepared and maintained in accordance with the environmental requirements specified by the supplier for the equipment. *Refer to risks: B-4, B-5, B-6, B-7*	B.2	Unauthorized use, disclosure, modification, or destruction of systems and data could occur.
4.9	Periodic inventories of computer hardware, data storage media, and supplies must be performed and reconciled. *Refer to risks: B-1,B-2,B-5*	B.3	Computer hardware may be used by unauthorized personnel to bypass normal security and operating controls and gain access to confidential systems and data.
4.10	Main computer consoles and network/system management terminals must be accessible to only authorized operations personnel and all console activity must be recorded. *Refer to risks: B-2, B-3*	B.4	Personnel may be subjected to unnecessary physical risk if environmental controls are not adequate.
4.11	Computer and network hardware must not be located in unsecured, high traffic areas. *Refer to risks: B-1, B-2*	B.5	Loss of critical data could occur due to improperly installed, maintained, or stored computer hardware and storage media.

	Standard of Control		Risk if Standard is Not Achieved
4.12	Fire detection, prevention, and extinguishing systems and equipment must be installed at computer hardware sites, accessible to operations personnel, and periodically tested. *Refer to risks: B-1, B-4,B-5,B-7*	B.6	Operational efficiency and reliability may be impaired and significantly disrupt processing.
4.13	All computer hardware must be protected against electrical surges, water damage, and natural disasters with the potential to disrupt operations. Refer to risks: B-1, B-4, B-5, B-7	B.7	Significant damage or destruction to computer hardware, software, and data could occur as a result of inadequate environmental monitoring and control systems.
4.14	Computer hardware sites must not be constructed or located near any combustible or hazardous areas. *Refer to risks': B-1, B-4, B-5, B- 7*		
4.15	Computer hardware sites must be kept clean and free from combustible materials. *Refer to risks: B-1, B-4,B-5,B-7*		
4.16	All computer hardware and software problems/errors must be recorded, monitored, and analyzed to ensure timely identification and correction. *Refer to risk: B-6*		

Computer Access Security

The objectives of computer access security controls include protecting the integrity and accuracy of computer data/programs and providing for the security and privacy of confidential/proprietary or sensitive data/programs.

	Standard of Control		Risk if Standard is Not Achieved
4.17	Custodians of computer equipment must ensure access security software is installed on the equipment when it is used for business, engineering applications, product testing and/or manufacturing processing. The access security software may be part of the computer operating system. At a minimum, access security software must perform the following functions:	C.1	SDLC information may be disclosed or lost, which may adversely affect the Company's competitive position.

	Standard of Control		Risk if Standard is Not Achieved
	a) Protect data files and programs from unauthorized access and/or alteration, theft, or destruction; *Refer to risks: C-1, C-2, C-3, C-4, C-8* b) Include access control facilities that provide a means to segregate incompatible business functions through the use of unique user ID/password verification; *Refer to risks': C-1, C-2, C-3, C-4, C-5, C-10* c) Automatically require passwords be established and changed in accordance to and within the time periods established by Corporate/Sector/Group policies. Passwords must be encrypted when stored and only decrypted during actual password validation processing; and *Refer to risks: C-J, C-2, C-3, C-4, C-8, C-9, C-11* d) Have the ability to automatically create audit trail transactions showing significant security events such as unauthorized access to application data files/programs and unauthorized access attempts to applications/transactions that are proprietary and subject to fraud, *Refer to risks: C-1, C-2, C-3, C-4, C-8, C-9*		
4.18	Custodians of computer equipment, in coordination with general and department managers, must appoint security administrators. The security administrator's function should be segregated from computer operations and systems development when practical. *Refer to risks: C-6, C-7*	C.2	Computers that process business, manufacturing, and engineering systems transactions, and that per-form product testing, may not have adequate access to security software.

	Standard of Control		Risk if Standard is Not Achieved
4.19	Security administrators, in coordination with general and department managers, must prepare and enforce security administration procedures. These procedures include: a) Establishing each new user account with documented management approval; b) Granting access to production data files and programs; c) Controlling the use of software procedures (privileges) that bypass normal access security controls; and d) Defining, reporting, and investigating unauthorized access attempts in compliance with Corporate/Sector/ Group policies. *Refer to risks: C-7, C-8, C-9, C-12*	C.3	Computer access security software or operating systems may not provide adequate minimum protective or detective security controls
4.20	Security administrators, in coordination with Corporate/Sector/Group Personnel Departments, must establish procedures to maintain or deactivate employee computer accounts upon the employee's transfer or termination from SDLC on a timely basis. Procedures must also be in place to detect active computer accounts assigned to terminated employees. *Refer to risks: C-13, C-14*	C.4	Passwords to user computer accounts may be disclosed and allow unauthorized access to data and programs.

	Standard of Control		Risk if Standard is Not Achieved
4.21	Application system owners must: a) Authorize access to the application and its data to appropriate users. Access should always be restricted on a "need to know" basis; *Refer to risks: C-1O, C-15* b) Classify data files and programs consistent with SDLC policy on Protection of Proprietary Information (POPI). The final decision as to classification rests with the General and department managers; *Refer to risks: C-1, C-11, C-15, C-16* c) Label computer-generated reports and on-line video screens containing confidential or sensitive information with the proper SDLC security classification (e.g., SDLC Confidential Proprietary, or SDLC Registered Secret Proprietary); and *Refer to risks: C-1, C-11, C-16* d) Confirm annually with user department management the continued need for user's access. The confirmation process should be conducted with the assistance of the computer equipment's custodian and security administrator. *Refer to risk: C-17*	C.5	Inadequate segregation of duties may result from the combination of system accesses and manual duties.
4.22	Department managers must ensure access granted to multiple systems does not compromise segregation of duties. *Refer to risks: C-10, C-17*	C.6	Computer access security controls may not be implemented.
4.23	Corporate/Sector/Group Controllers or General Managers or Directors and IS Directors must approve the implementation of electronic data transfer systems, such as invoices, orders, or payments between SDLC and suppliers, customers, or contract services. *Refer to risks: C-1, C-18*	C.7	Security administrators may have conflicting duties that would allow them to both change access security and system processing.

	Standard of Control		Risk if Standard is Not Achieved
4.24	Computer systems or programs are considered in production status if systems/programs are relied upon by management for conducting, recording or reporting business, engineering or manufacturing operations. Software for production systems may be developed by IS departments, end users or vendors. Production systems may operate on mainframe, departmental, personal computers or wide-area/local-area networks. The following controls must exist to protect production computer software and data files: a) Application programmers must not be provided with permanent update access to production software or data files. Management must grant specific authorization to programmers to change production software or data files to correct system failures; and b) Update access to production software or data files, that are classified SDLC Confidential Proprietary or Registered Secret Proprietary, by computer operations personnel or programmers, who maintain or execute computer operating systems and/or system management software, must be logged. Management must designate an appropriate individual to maintain records evidencing timely review of these logs. *Refer to risks: C-J, C-1J, C-15, C-16*	C.8	Access to production data files and programs may be granted without proper authorization.

	Standard of Control		Risk if Standard is Not Achieved
4.25	Suppliers, contract programmers and C-9 other non-SDLC staff must sign non-disclosure agreements before they are given direct access to SDLC computer systems. Non-SDLC staff who use SDLC computer systems must have separate and unique computer accounts or user lDs. *Refer to risks: C-1, C-11, C-15, C-16*	C.9	Unauthorized access attempts may be made on a regular basis without detection.
4.26	Custodians of computer equipment must ensure virus detection software is installed on the equipment when it is used for business, engineering applications, product testing and/or manufacturing processing. *Refer to risk: C-19*	C.10	Access to multiple systems by the same user could result in an improper segregation of functions.
		C.11	Sensitive information may be accessed and/or disclosed to unauthorized personnel.
		C.12	Special access privileges may be granted which result in unnecessary or unauthorized access to production data files.
		C.13	Terminated/transferred employees may gain access to and/or damage sensitive SDLC data, disrupt normal business processing, or disclose sensitive information to outsiders.
		C.14	System access by terminated/transferred employees or accounts assigned to terminated/transferred employees may not be detected.
		C.15	System users may be given access to data files and programs that are not required for their job functions.
		C.16	Proprietary information stored on computer systems may not be properly protected.
		C.17	Users may change job responsibilities but not change their system access requirements.

	Standard of Control		Risk if Standard is Not Achieved
4.27		C.18	Business data may be transmitted without proper data processing or accounting controls resulting in erroneous orders, payments, or purchases.
4.28		C.19	Business, manufacturing or engineering systems may become dysfunctional, resulting in productivity and revenue losses, or critical data could be destroyed.

Network Security

The objectives of network security controls include protection from unauthorized entry, misuse or alteration of information, and denial of service. SDLC networks are managed within three Tiers. Tier I, a SDLC Corporate organization responsibility, consists of the Wide Area Network (WAN). Tier II, a Group/Sector organization responsibility, is referred to as the Facility Backbone Network CFBN) and provides standards based connectivity between Tier III LANs and the Tier I WAN. Tier III, a local department responsibility, is referred to as the Local Area Network CLAN).

	Standard of Control		Risk if Standard is Not Achieved
4.29	Custodians of data processing equipment who operate communications networks must document and maintain descriptions of their network topology. *Refer to risk: D-1*	D.1	SDLC proprietary information may be disclosed or lost, which may adversely affect the Company's competitive position.
4.30	Standards based protocols must be used whenever they are available. Only tested and approved protocols will be allowed over SDLC networks. *Refer to risks: D-2, D-3*	D.2	Data may not be accurately or completely transferred.
4.31	Network managers must utilize configuration, performance, fault, accounting, and security management tools to monitor networks. *Refer to risks: D-l, D-2, D-3, D-4, D-6, D-7*	D.3	Transmissions may not have adequate error correction.
4.32	Network addresses and names must be obtained and maintained as specified in the SDLC Data Network architecture (CDNA) standards. *Refer to risks: D-2, D-3, D-7*	D.4	Sensitive information may be accessed and/or disclosed to unauthorized personnel.

	Standard of Control		Risk if Standard is Not Achieved
4.33	Custodians of computer equipment must make data encryption facilities available to protect data transmission of proprietary information. Passwords must be encrypted during network transmission. *Refer to risks:* D *I, D-4, D-5*	D.5	Proprietary information stored on computer systems may not be properly protected.
4.34	Internal access to SDLC networks must be controlled by single factor authentication (e.g., a unique user ID and password or token authentication). *Refer to risks: D-1, D-4, D-5*	D.6	Proprietary data may be disclosed to unauthorized personnel during transmission.
		D.7	Data bases may not contain accurate and complete information after system failure.

Systems Development Methodology

	Standard of Control		Risk if Standard is Not Achieved
4.35	Corporate/Sector/Group departments responsible for software development and maintenance must define and document standard methodologies that must be used in developing and maintaining application systems. *Refer to risks: E-l,E-2, E-3, E-4*	E.1	Systems may be implemented which do not meet user requirements or comply with SDLC software quality standards.
4.36	Corporate/Sector/Group system development methodologies must include the following components: a) Systems development projects must be segmented into measurable parts or phases with predefined deliverables; *Refer to risks: E-1, E-3* b) Project team roles and responsibilities must be clearly defined and documented; *Refer to risks: E-2, E-4* c) The system development project team, consisting of user, IS, and application owner personnel, must approve the completion of each major phase of development prior to progression to subsequent phases; and *Refer to risks: E-3, E-4, E-5, E-6*	E.2	Roles and responsibilities may be unclear, resulting in increased development cycle times or system inadequacies
	d) Formal plans must be prepared for E-5 system development projects. Development and project plans must comply with the SDLC Quality Policy for Software Development and include the following attributes at a minimum: -A clear and accurate statement of business purpose and requirements for the proposed system; *Refer to risks: E-2, E-5, E-6* -A feasibility study identifying possible software solutions and cost/benefit analysis; *Refer to risk: E-5* -A detailed logical and physical system design; *Refer to ris.k: E-6*	E.3	Systems may be implemented without approval of the system design, proper testing, or conversion resulting in erroneous processing.

Standard of Control		Risk if Standard is Not Achieved
-System and user acceptance testing that will adequately test each system function and condition defined by the detailed logical and physical design; *Refer to risks: E-7, E-8* -Specifications for conversion to the proposed system that will ensure the integrity of processing procedures and data; *Refer to risk: E-9* -Preparation of user procedures that document how users interact with the system and how that interaction is controlled. User procedures should reasonably answer questions on system operation, error correction, and control; *Refer to risks: E-10, E-11* -Preparation of operations documentation that details how to operate the application system. The documentation should include procedures for restarting the application in the event of hardware or software failure; and *Refer to risks: E-12, E-13* -Training to sufficiently enable users E-12 to independently operate and control system processing. *Refer to risk: E-14*	E.4	Users may not actively participate in the development process, which could result in-incorrect decisions during the design and testing phases.
	E.5	Improper selection of data processing solutions to business problems may result from incomplete evaluation of alternatives.
	E.6	The system design may not be properly documented and communicated resulting in uncontrolled or erroneous processing.
	E.7	Individual programs and the entire system may not be adequately tested or may not operate as intended resulting in erroneous processing.
	E.8	Users may not participate in acceptance of the system. The system may not operate properly and may not meet their needs.
	E.9	Data files may not be properly converted to the new system.
	E.10	Users may not be able to recover from processing errors.

	Standard of Control		Risk if Standard is Not Achieved
		E.11	Users may not be able to process independently of IS or other personnel who developed the system.
		E.12	Operations personnel may not be able to operate the system.
		E.13	Operations and/or user personnel may not be able to recover from errors to continue business processing.
		E.14	Improperly trained users may not be able to adequately operate and control the system.

Configuration Management

Changes to the production environment, including software, hardware, and operating procedures, must be authorized, documented, and tested.

	Standard of Control		Risk if Standard is Not Achieved
4.37	Requests for changes to the production environment must include a business purpose or business impact analysis, and must be approved by the system owner. *Refer to risks: F-l, F-2*	F.1	Erroneous changes or changes resulting in improper use of the system may result from unauthorized system changes.
4.38	Changes to the production hardware and/or software environment must be tested. Tests must include sufficient conditions to ensure the new system configuration operates as intended. Testing must also include evidence that all requirements were tested to the satisfaction of the ultimate users of the system. *Refer to risks: F-3, F-4, F-5*	F.2	Programmers or other personnel preparing the system change may not adequately evaluate the impact of the change on business processing.
4.39	If the system change will result in the creation of journal entries or changes in journal entry account distribution, the change must be approved by financial management. *Refer to risks: F-5, F-6*	F.3	Changes may not be properly tested and their implementation may result in erroneous system processing.

	Standard of Control		Risk if Standard is Not Achieved
4.40	Organizations or departments with responsibility for hardware or software must document and implement plans and procedures for Software Configuration Management. Software Configuration Management includes program change control, version and release management, status reporting, and changes to the operating system software. *Refer to risks: F-2, F-4*	F.4	Users and operations personnel may not be aware of system changes that could result in erroneous system processing.
4.41	Organizations or departments with responsibility for hardware or software must follow an approved, documented System Development Methodology when making maintenance changes to the production environment. *Refer to risks: F-4, F-7*	F.5	Financial or operational records may be misstated.
4.42	If distributed systems are designed with multiple copies of the same programs and data files on more than one computer, system-wide version controls must be developed to ensure proper versions of programs and data files are used throughout the system. *Refer to risks: F-1, F-3*	F.6	Improper journal entries or account distribution may result from the system change.
		F.7	Users and operations personnel may not be able to recover from system failure.

Computer Operations and Backup

Organizations or departments that operate computer equipment are responsible for ensuring that computers are operated in accordance with SDLC policies and procedures.

	Standard of Control		Risk if Standard is Not Achieved
4.43	Computer data files, programs, and system software must be backed up periodically to ensure continuity of business operations in the event of a hardware or software failure. *Refer to risks: G-l, G-2*	G.1	Programs and information assets could be lost due to hardware or software failure, or human error.

	Standard of Control		Risk if Standard is Not Achieved
4.44	Corporate/Sector/Group Controllers are responsible for identifying data files that must be retained to comply with regulatory or statutory requirements, such as taxing authorities or government contracting agencies. *Refer to risks: G-3, G-4*	G.2	Tape files could be lost or erased in error.
4.45	Owners/Custodians of computer systems must maintain a system to record and track backup data files and other off-line media for recovery and retention purposes. *Refer to risk: G-5*	G.3	Business data files may not be properly retained and could subject SDLC to fines and penalties.
4.46	Backup information, including programs, data files, and supporting documentation, must be maintained at an off-site location not subject to the same peril as the normal computer processing site. *Refer to risks: G-6, G-7*	G.4	Data files retained for regulatory requirements may not contain complete and accurate data.
4.47	Personnel responsible for computer operations must prepare and maintain policies, procedures, and instructions on the operation of the computer and system software. *Refer to risk: G-8*	G.5	Backups may not be available and procedures may not be operating as management intended.
		G.6	In the event of a disaster, critical files may be destroyed that could prevent recovery of business processing.
		G.7	The ability to continue business operations in the event of an emergency may be impaired.
		G.8	Procedures for the operation and control of computer systems may not be properly communicated or performed.

Disaster Recovery Plans

The objective of disaster recovery planning is to ensure the continuity of SDLC's business, engineering and manufacturing operations in the event of unanticipated computer processing disruptions such as operational failures or site disasters that destroy or prevent access to the computer equipment, data, and software.

	Standard of Control		Risk if Standard is Not Achieved
4.48	The custodians of computer applications, equipment and facilities, in coordination with application system owners, are responsible for arranging for alternative equipment and/or computing facilities. Alternative equipment or facilities should be adequate to recover critical on-line, batch processing and network systems. Disaster recovery plans must include the following: a) A determination of the most effective alternative processing method for both critical and non-critical applications. Alternatives include: -Processing at another SDLC site; -Processing at an alternative computer site using a reciprocal agreement with another company or a conditional site maintained by a recovery site vendor; or -Not processing applications until computer equipment and or sites are restored; b) A plan detailing IS and user personnel requirements and special skills needed in the event of an unanticipated pro-cessing disruption; and c) Storage of critical replacement forms, supplies, and documentation at off-site storage, preferably a vendor's warehouse. *Refer to risks: H-l, H-2, H-3, H-4*	H.1	SDLC may incur a severe disruption of business, engineering, or manufacturing operations if computer equipment custodians are not able to recover in the event of an unanticipated processing disruption.

	Standard of Control		Risk if Standard is Not Achieved
4.49	Application system owners must classify their application's recovery priority. This priority must be used by computer equipment custodians to determine the sequence of restarting critical application systems in the event of an unanticipated processing disruption. The priority assessment should include the following: a) Quantify the risk in terms of dollars, production volume, or other measurable terms due to partial or total loss of processing the application; b) Assess the lead time between loss of application processing and adverse impact on SDLC operations as part of determining acceptable down time; and c) Obtain agreement from Sector/Group/ Division management on the classification as to critical or non-critical. *Refer to risks: H-1, H-2, H-3*	H.2	Critical systems may not be recovered first.
4.50	Detailed disaster recovery plans must be documented and tested periodically to ensure recovery can be accomplished. Where tests of the full disaster recovery plans are found to be impractical due to business conditions or the cost of testing, test plans must be developed and implemented to test portions of the plan. *Refer to risks: H-l, H-4*	H.3	SDLC could sustain substantial financial loss if critical computer systems and equipment were severely damaged or destroyed.
4.51	Custodians, in conjunction with application owners, must review and update the disaster recovery plan annually. Updates should reflect changes in applications, hardware and/or software. *Refer to risk: H-4*	H.4	The disaster recovery plans may not be effective.

Application Systems Control

Application system controls are concerned with the integrity, accuracy, and completeness of data input to, and processed, stored, and produced by, the application system.

	Standard of Control		Risk if Standard is Not Achieved
4.52	All manually input or interfaced transactions must be properly originated and authorized and include evidence of authorization prior to processing. *Refer to risks: I-1, I-2*	I.1	Unauthorized transactions may be processed.
4.53	Manually input or interfaced data must be subjected to sufficient edits and validations, including duplicate and completeness checks, to prevent or detect data input errors. *Refer to risks: I-1, I-2*	I.2	Invalid or erroneous data may be processed and affect operating and/or financial decisions.
4.54	Manually input or interfaced data rejected by application system edit and validation procedures must be controlled to ensure that input errors are identified and corrected, and data is re-input to the system on a timely basis. *Refer to risks: I-3, I-6*	I.3	Rejected input may not be corrected and re-input into the system resulting in incomplete processing.
4.55	Application systems must provide an audit trail from the input transactions recorded by the system to the source transaction and originating user or system. *Refer to risks: I-4, I-5*	I.4	An adequate audit trail may not exist to provide a means of substantiating input transactions.
		I.5	Financial and/or operating personnel may not be able to explain transaction activity or account balances.
		I.6	Untimely correction of rejected items may result in incorrect records and financial statements.

Processing Controls

	Standard of Control		Risk if Standard is Not Achieved
4.56	Application systems and/or manual user procedures must include control procedures that ensure: a) All business transactions have been input and accepted by the system and processed completely, accurately, and timely; *Refer to risks: J-1, J-2, J-4* b) Proper accounting cut-off of transactions has been made between accounting periods; and *Refer to risks: J-4, J-5* c) Business transactions passed from one application system and processed by another system have been properly passed from the source system and received and processed by the receiving system. *Refer to risks: J-2, J-4, J-6*	J.1	Users may not have assurance that all transactions have been properly processed.
4.57	Developers of applications systems must prepare specific procedures to restart processing in the event of temporary hardware or system failure. These recovery procedures must be provided to the personnel responsible for operating the system. Application restart/recovery provisions, whether automated or manual, must be developed to enable proper re-synchronization of applications, data, and files, upon recovery from system error or failure. *Refer to risks: J-3, J-4*	J.2	Transactions may not be properly passed from one system to another
4.58	Computer resources must be sufficient to enable timely on-line response and information processing. *Refer to risks: J-1, J-5*	J.3	Personnel operating the system application may not be able to restart/recover processing in the event of hardware or software failure.
		J.4	SDLC financial statements may be misstated.
		J.5	Financial or operational reports may not be complete and include all appropriate business transactions.
		J.6	Transactions may not properly update files.

Output Controls

	Standard of Control		Risk if Standard is Not Achieved
4.59	Application systems must provide activity logs which evidence: a) All input transaction data, including data received from other systems; b) Additions or changes to master file or reference table data; and c) Internally generated transactions. R*efer to risks: K-1, K-2, K-3*	K.1	Application systems may not produce adequate audit trail, input, or processing reports to control processing.
4.60	Application system audit trails should provide for unique identification of processed transactions to allow them to be traced and vouched through the system. *Refer to risks: K-l, K-2, K-3*	K.2	Erroneous or unauthorized changes to system data may not be detected.
4.61	All on-line video screens or reports should include sufficient information to ascertain their origin, period covered, contents, and completeness, as well as their POPI classification. *Refer to risks: K-l, K-2, K-3, K-4*	K.3	System audit trails may not be adequately generated or maintained
4.62	Data processing custodians and application system users must establish and implement procedures to ensure that proprietary reports are promptly collected by authorized users, and that remote printers or report distribution sites are secured. *Refer to risk: K-4*	K.4	Proprietary information may be unintentionally disclosed to the detriment of SDLC.
4.63	Data files, data storage media, and computer reports (including carbons and fiche) containing proprietary information must be properly destroyed after their useful lives. *Refer to risk: K-4*	K.5	

Paperless Transaction Processing and EDI

Paperless transaction processing refers to a business operation in which electronically processed or stored information replaces the traditional paper trail of evidence. Paperless processing control provisions, like those for a manual-processing environment, are concerned with the authorization, accuracy, and completeness of transactions. Thus, all relevant business cycle and application controls apply.

	Standard of Control		Risk if Standard is Not Achieved
4.64	Paperless transactions must include evidence of proper authorization. Effective logical access and security administration control must be in place to ensure reliance upon electronic authorization. *Refer to risk: L-1*	L.1	Transactions may not be legitimate, introducing the risk of fraudulent processing and legal liabilities.
4.65	Controls must be in place to ensure the authenticity of the transaction source. The minimum authentication and security requirements must be defined by business areas and their customers. *Refer to risk: L-2*	L.2	Transaction authenticity or integrity may not be assured, decreasing the reliability of the information and also introducing the risk of fraudulent or erroneous processing.
4.66	The content of paperless transactions must not be altered through the transmission process, i.e. from point of origination to receipt. Each component in the paperless processing system, from manual entry and computer operations to application edits and system security, must encompass the controls necessary to ensure transaction integrity. In addition, there must be adequate audit trails at key points in the transmission path. *Refer to risk: L-2*	L.3	Paperless records may not be retained, or securely held, thus introducing risk of information loss and possible regulatory penalties.
4.67	Retention of paperless transactions must be managed to ensure that the electronic records are available, authentic, and reliable and reproducible. Retention must be in compliance with Corporate/Sector/Group retention policies and schedules. *Refer to risk: L-3*	L.4	Responsibilities may be unclear, causing SDLC to be unnecessarily liable for system failure or transaction loss.

	Standard of Control		Risk if Standard is Not Achieved
4.68	For EDI-based processes, Trading Partner Agreements (TPA's) must be prepared and approved by Corporate/Sector/Group legal departments prior to the initiation of ED! processing. TP A's should identify the specifications for transaction processing as well as trading partner responsibilities, terms and conditions, and corresponding liabilities. *Refer to risk: L-4*	L.5	
4.69	Where Value-Added Networks (VAN's) are utilized, operational, security, and legal liabilities for the integrity of SDLC information must be contractually defined. *Refer to risk: L-4*	L.6	

SECTION 5: FORMS

- None at this time

SECTION 6: EXCEPTIONS

- None at this time

SECTION 7: TOOLS/SOFTWARE/TECHNOLOGY USED

- None at this time