

EDI Systems Audit Program

A	<i>Planning/Administrative</i>		
1	Review the Letter of Understanding and create the APM (Audit Planning Memorandum) accordingly.	A-1	DB 02/03
2	Gain a high-level understanding of Auditee's EDI environment through discussions with Auditee IT Management and prepare a detailed audit program.	A-2	DB 02/03
3	Prepare detailed client assistance list and send it to Auditee.	A-3	DB 02/03
B	<i>Management & Organization</i>		
	Review EDI management documents for evidence of executive commitment and sound business strategy		
1	Review and comment on the EDI Business Plan		
2	Determine level of participation in EDI industry groups		
3	Review for evidence of long term proactive EDI business planning	Covered	
4	Obtain evidence of cooperative project management and relationship building with trading partners	Covered	
5	Assess viability of EDI compliance program or control self assessment program	Covered	
	Assure the system development lifecycle procedures require the testing and review of new EDI technology controls		
6	Assure contractual arrangements with trading partners and software/network vendors are well documented and reviewed by legal counsel.		
C	<i>Application Level Accuracy and Completeness</i>		
1	<i>Translation Software</i> <ul style="list-style-type: none"> • Verify translation software is capable of performing required syntax checking • Review test base cases and testing procedures (run own tests if required) 	Need more info	
2	<i>Acknowledgement Levels</i>		

	<ul style="list-style-type: none"> Review criteria for various levels of acknowledgement Verify they are agreed to by the trading partner(s) 	Need more info	
3	<p><i>Special Editing Rules for Positive or Negative Acknowledgement</i></p> <ul style="list-style-type: none"> Verify effective documentation exists for special editing rules critical to positive or negative acknowledgment. Verify special editing rules are tested. 	Need more info	
4	Assess the adequacy of application input/edit controls.	Need more info	
5	Verify completeness controls are built into the transaction process		
6	In the event of normal edit failure, identify imbedded audit modules used as triggers and warnings.		
7	Verify the translation software correctly matches headers and trailers at: <ul style="list-style-type: none"> The interchange, functional group level The application level 		
8	Review controls outside the translation software, e.g., number and value batching		
9	Review controls outside the translation software implemented by trading partners.		
10	Verify procedures for reporting irregularities are well-documented and followed		
11	Verify common procedures for error/exception handling are well-documented and followed		
12	Verify audit/management trails contain sufficient information to prove existence and evidence of a transaction		
	Suggest a management letter of compliance be exchanged between trading partners to confirm continuous operation of controls		
C	<i>Environmental Level Accuracy and Completeness</i>		
1	<p><i>Change Control</i></p> <ul style="list-style-type: none"> Verify program change control procedures: <ul style="list-style-type: none"> Exist Are standardize Are synchronized between trading partners Verify change control documentation is maintained 		

2	Review test results for: <ul style="list-style-type: none"> • Message acknowledgement • Security features • Special edits 		
3	Review the segregation of duties between EDI application development, application administration, and security audit & control		
4	Verify virus protection assurances offered by vendors of EDI software		
5	Obtain an audit report from the VAN Network vendor's auditors if possible		
6	Trading Partner Agreements <ul style="list-style-type: none"> • Verify trading partner agreements <ul style="list-style-type: none"> ○ Exist ○ Have been approved by competent legal council, e.g. clauses regarding electronic signatures ○ Clearly define liability for errors ○ Set out migration procedures to new versions of standards 		
7	Verify VAN network contracts include: <ul style="list-style-type: none"> • A clause on "confidentiality guarantee" • A clause on "statement of reliability" • A clause on "guaranteed performance" 		
8	Verify EDI software agreements include: <ul style="list-style-type: none"> • A clause on "confidentiality guarantee" • A clause on "statement of reliability" • A clause on "guaranteed performance" 		
D	Security		
1	Verify authorization controls are functioning as required		
2	Check adequate consideration was given to encryption/MACing/digital signatures for security messages		
3	Where data is transmitted across public connections (Internet & wireless): <ul style="list-style-type: none"> • Obtain detail regarding implemented connections • Ensure secure identification and authentication occur • Ensure proper authorization is applied and access authorities granted to third party systems and users does not exceed what is required for the intended purpose • Assess the risk introduced to the network, as a whole, by the current connection service and security features 		

	<ul style="list-style-type: none"> • Ensure monitoring is in place 		
4	<p>Where encryption is used:</p> <ul style="list-style-type: none"> • Check appropriate algorithm is used such as 3DES or RSA, and sufficient overhead is available to handle the encryption process • Where digital signatures or MACing is used check coverage is “end to end” through the network • Verify key management procedures are documented and adequate: • Check key values are <ul style="list-style-type: none"> ○ Randomly generated ○ Used for a single purpose ○ Keys are exchanged and used by key custodians according to principle of dual custody and split knowledge 		
4	Check there is adequate and timely follow-up of security incidents		
5	Verify there are documented security incident escalation procedures and check their compliance.		
6	Verify physical and logical security of terminal, telecommunication components and work areas		
E	<i>Auditability</i>		
1	Review a sample of logs from the required retention period and verify they contain the data sets specified in the control procedures		
2	Test access controls over electronic authorization facilities to determine they function as specified		
3	Review and evaluate the adequacy of testing integrity controls in EDI system under development		
	Test integrity controls both pre- and post-implementation		
	Test concurrent monitoring modules in a test environment – if audit embedded monitors – consider control in the production environment (source/object code comparison)		
	Review output from concurrent monitoring modules prior to reporting an opinion on managements statement of continuous compliance		
F	<i>Timeliness and Recoverability of a Systems Outage</i>		
1	Review procedures relating to a failed communications line and ensure roles and responsibilities for each trading partner and other participants are mutually defined		
2	Observe or review the documented results of the testing of contingency		

	plans (disaster recovery & business continuity) for system outages – follow up exceptions		
3	Verify validity of assumptions for maximum tolerable outages and discuss with management		
4	Verify trading partners agreement specifies periodic interval for testing continuity plans and evidence of testing		
5	Check time required to back out from outage is adequate		
6	Determine physically compatible hardware is on site or can be replaced within an agreed time frame		
7	Review recovery procedures for adequacy		
8	Check EDI operators familiarity with the recovery procedures		
9	Determine whether EDI system software upgrades have been made		
10	Verify backups were made		
11	Verify sample of EDI backup transaction media to ensure correct cycle is maintained and media correctly hold those transaction		
12	Check installation backup contingency planning procedures are documented and tested.		
13	Obtain list of EDI problem report. Check items in section relating to outages were correctly followed up and resolved		
F	<i>Timeliness and Recoverability of Failed Transaction Set</i>		
1	Verify requirements and conditions with regards to tracing requests are defined and followed		
2	Ascertain if retention requirements consider whether there is sufficient time for error correction and resolution disputes		
3	<i>Trading Partner Agreements</i> Check trading partner agreements cover requirements for: <ul style="list-style-type: none"> • Exception reporting • Reporting of items (such as negative functional acknowledgements, MACing failures, etc.) 		
4	Verify incidents will remain reported for at least one year		
5	Verify members have facility to report trading partners who seem to encounter repetitive problems		

6	Verify requirements for reversal of transactions are well-defined		
G	<i>Third-Party Network Providers</i>		
1	Review independent audit report findings		
2	<p><i>Third-Party Network Provider Agreements</i> Verify agreements with third-party network providers define their responsibilities for:</p> <ul style="list-style-type: none"> • Continuous service in case of a disaster • Service guarantees • Provision of manual fall-back procedures • Recovery of lost messages • Identification and follow-up of errors and inconsistencies in a timely manner • Confidentiality of the trading partner information • Confirmation of the customer’s absolute right to data in case of disputes • Justification of all billings • Requirements for adding and deleting partners and transactions • “Right to audit” clause 		
3	Verify the VAN retains a log of transactions for a specified period of time		
4	Verify reports from third-party network providers are reviewed for accuracy and errors/omissions are followed up separately		
5	Ensure use of third-party audit transactions are being used where applicable		

N	<i>Reporting and Review</i>		
	Prepare draft Issues Matrix.		
	Meet with Auditee management on the last day of fieldwork to discuss the issues and verify their factual accuracy.		
	Prepare the Summary Memorandum (SM).		
	Prepare work papers for review and organize electronic files.		
	Complete detail review and sign-off.		
	Complete engagement partner review and sign-off.		
	Complete partner/QA review and sign-off.		
	Finalized Issues Matrix and provide to Pittston IT Internal Audit Management.		