

## EXHIBIT C - EVALUATION OF CONTROLS IN INFORMATION SYSTEMS (IS)

The evaluation of internal controls of a company's information systems (IS) is a critical element of the examination process. Determining the complexity of a company's IS environment; and, determining the extent of work that must be performed to evaluate the controls of the system is not always easy. Knowledge gained about systems during previous examinations may no longer be relevant if systems have been refreshed and replaced. But requesting a company complete the full Information Systems Questionnaire (ISQ) may not be the most effective and efficient approach to evaluating IS controls, especially if other external auditors or other state examiners have recently completed a systems control review upon which some reliance can be placed.

The Information Systems Planning Questionnaire (ISPQ) is a tool designed to assist the examiner in planning the extent of IS control work that may be necessary on an examination. The ISPQ provides the department of insurance with a high-level overview of the company's information systems environment. It is used to plan the scope and extent of IS control work to be performed and assist the examiner in determining whether all or only partial sections of an ISQ should be prepared for the examination. The examiner should review the company's responses and assess the examination difficulty with respect to information system control testing. To achieve maximum benefit the ISPQ should be completed in advance of even normal examination planning so that the examiner can begin planning what, if any, sections of the full ISQ the examiner will complete.

**NOTE:** The following questions are included in both the ISPQ and the ISQ. If the ISPQ is utilized and subsequently it is determined to complete a full ISQ, the repetitive questions in the ISQ should be removed to avoid redundancy.

Information Systems Planning Questionnaire (ISPQ)	Information Systems Questionnaire (ISQ)
2a	Attachment A
4a	A4
4b	A2
4c	A1
5	A7
6	B1, B23, B25, I8, G12
7a	D1
8	Scoping Note for Section I
9a	G12
9b	Attachment B
10a	E1, E8
10c	E1

# INFORMATION SYSTEMS PLANNING QUESTIONNAIRE (ISPQ)

For the questions below, provide the requested documentation and the name, title, telephone number and e-mail address of the individual who will be most able to discuss and clarify the information presented.

If a particular section does not apply to your company, give a brief explanation why it does not apply. All responses should be in the form of a separate summary memorandum headed with the corresponding section label. Where possible, electronic responses are preferred.

## 1. Information Systems

If the company does not process its business electronically, provide a narrative description explaining how the company's business is processed. The remainder of this section does not need to be completed.

If the company only processes business electronically on a stand-alone personal computer and does not use networking technology, provide a narrative description explaining how business is processed, including the type of application software being used. The remainder of this section does not need to be completed.

## 2. Information Systems Infrastructure

- a. Provide a listing of the locations of all data processing centers used by your company, whether owned by the company or by a third-party administrator that processes data for the company.
- b. Provide a system-wide map or topography, showing all hardware platforms and network connections indicating all internal and external access points. In addition, complete a separate Systems Summary Grid for each platform (see Attachment 1). A sample Systems Summary Grid is provided with this survey (see Attachment 2).
- c. Provide a narrative explanation of the application-level interfaces among the various programs/platforms (e.g., claims system feed into the accounting system).
- d. Provide the name, telephone number and e-mail address of the individuals holding the following positions in the company, if they exist: Chief Information Officer, Chief Technology Officer, Chief Security Officer, and System Architect.

## 3. Financially Significant Systems

If you use multiple platforms/systems to process premium, claim or reinsurance transactions, include a reconciliation of amounts processed on each separate system to total dollar amount processed during the prior year. Indicate whether you anticipate any change in processing volumes during the current year.

## 4. Information Technology Governance

- a. Provide specific detailed organizational charts for the company's Information Systems Division and its various functional divisions (e.g., show operations, programming, support services, etc.). Show reporting relationship of the Information Systems Division within the organization.
- b. Provide an executive overview of your company's IS strategic plans, including plans for e-commerce.
- c. Provide an executive overview of your IS Steering Committee or other group, that establishes and directs IS policies and strategies, indicating the membership of the group and the frequency of their meetings.

## **5. Information Systems Audits/Reviews**

- a. Provide a list of any Information Systems audits/reviews performed within the last two years, including e-commerce areas. Include the dates, review subjects and who performed the audits/reviews (e.g., Internal Audit, CPA, SAS70, Sarbanes-Oxley, State Departments of Insurance, governmental agencies and any other contractor or affiliate who may have performed and audit/review.)
- b. Provide the name, phone number and email address for the partner of your company's independent CPA audit team and the internal audit director, if they exist.
- c. Provide the name and trading symbol of the parent holding company if your company belongs to a group that files with the SEC.

## **6. Information Systems Security**

Provide a copy of your Information Systems Security Policy, including e-commerce. If no formal written policy exists, provide a detailed description of the security features in place and functioning at all levels, both physical and logical. Also, include any anti-virus/anti-malware software, intrusion detection systems, and patch management systems used and the strategy for keeping these products current.

## **7. System Development/Change Management**

- a. Provide an executive overview of the company's system development life cycle (SDLC) and change management methodologies and indicate whether the company uses internal personnel and/or external vendors to develop or change its systems or programs.
- b. Provide the name, vendor and version number for all change management/system development software, if utilized.

## **8. E-Commerce**

**Note:** E-Commerce methods of transmission may include voice recognition units (VRUs), the Internet, third-party extranets and wireless and broadband communications media.

Describe whether the company is conducting any business through e-channels, indicating the type and volume of business and the date when it was implemented.

## **9. External Services/Outsourcing**

- a. Provide a list of any business or data processing services provided by the company to any other entities, including affiliates, indicating the type of service provided and a summary of the terms of the agreements (e.g., named parties, effective date, period and services covered.)
- b. Provide a list of any business or data processing services performed by any other entities on behalf of the company, such as a third-party administrator (TPA, MGAs, GA, etc.) or an affiliate, indicating the type of service provided and a summary of the terms of the agreements (e.g., named parties, effective date, period, location and services covered.)

**10. Business Continuity**

- a. Provide a copy of your Information Systems Business Continuity and Disaster Recovery Plans, including information on any contracts for alternate sites (i.e., named parties, site location, type of site, effective date and period covered). Also, provide evidence of the last test results for the plans and management's resolutions of any test discrepancies.
- b. Provide a description of your company's data and systems backup strategy, including your records retention policy.
- c. Provide a copy of the business impact analysis.

## Information Systems Planning Questionnaire (ISPQ)

### Attachment 1

### Systems Summary Grid

*For each primary hardware platform, list the application software products used in each of the insurance business cycles.*

Hardware Platform (manufacturer/model)					
Operating System					
Access Control Software					
Program Management Software					
Database Management Software					
Processing Location					
Individual Responsible					
Cycle/Application	Product Name and Version	Software Source: Developed internally; Purchased not modified Purchased customized Outsourced/service center	Developer/Vendor	Date of Initial Implementation	Date of Last Significant Update
Premium (policyholder management)					
Loss and Benefit (tracking and reserving)					
Financial Reporting (general ledger and accounting)					
Investments					
Reinsurance					
Agent Balances/Commissions					

**NOTE:** Make as many copies of this System Summary Grid as are necessary to represent every primary hardware platform being used at your company. These hardware platforms may include mainframe, minicomputer and/or network server systems.

## Pre-Examination Planning Survey

### Attachment 2

### Systems Summary Grid — Sample

*For each primary hardware platform, list the application software products used in each of the insurance business cycles.*

Hardware Platform (manufacturer/model)	IBM AS/400 Model 840				
Operating System	OS/400 v4r3				
Access Control Software	OS/400 and Client Access/400				
Program Management Software	Job Scheduler for AS/400				
Database Management Software	DB2 Universal Database for AS/400				
Processing Location	Company's home office				
Individual Responsible	John Smith, VP - Underwriting				
Cycle/Application	Product Name and Version	Software Source: Developed internally; Purchased not modified Purchased customized Outsourced/service center	Developer/Vendor	Date of Initial Implementation	Date of Last Significant Update
Premium (policyholder management)	PMS v6r2	Developed internally	By company, using Cobol, C++	09/1987	10/1999
Loss and Benefit (tracking and reserving)	Not on this platform				
Financial Reporting (general ledger and accounting)	Not on this platform				
Investments	Not on this platform				
Reinsurance	Not on this platform				
Agent Balances/Commissions	PMS v6r2	Developed internally	By Company, using Cobol, C++	09/1987	10/1999

**NOTE:** This page is for informational purposes only — it does not have to be returned with your survey response.

## EVALUATION OF CONTROLS IN INFORMATION SYSTEMS (IS) QUESTIONNAIRE

**INSTRUCTION NOTE 1:** In order to expedite the IS controls evaluation process, this questionnaire is designed to be completed by the insurance company's information systems management before the IS specialist(s) assigned to the examination begin(s) fieldwork. Accordingly, the tone of the questionnaire is directed to the insurance company's IS managers. The examiners recognize the wide variation in the size (e.g., large mainframe vs. small network) and structure (e.g., centralized vs. decentralized) of the many processing environments in place at companies throughout the insurance industry. Therefore, several sections of the questionnaire contain a "Scoping Note," which is designed to be answered by the insurance company's IS managers and evaluated by the examiner to determine whether or not the particular section of the questionnaire needs to be completed by the company and tested by the examiner. For those sections that will be completed, the answers to each question should be made in a manner that reflects an understanding of the company's particular control environment, as well as an understanding of the audit intent of each question. This can generally be achieved if the company involves an internal information systems auditor in the question answering process. Specific "Guidance Points" have also been included in the more technical areas of the questionnaire to help facilitate its completion by the company's IS managers.

**INSTRUCTION NOTE 2:** Every question includes a description of particular test documentation that should be provided by the insurance company. In those cases where documentation does not exist or is not otherwise available, the insurance company should provide examples of processes that can be observed and/or the individuals who can be interviewed to corroborate the presence of controls that are not formally documented.

**INSTRUCTION NOTE 3:** Due to the inherently high degree of change in information technology, the period under review for this questionnaire should generally range from the latest 12 to 24 months of the overall financial condition examination time period. The period under review should generally encompass the last year of the examination period and the period of time up to and including the actual examination fieldwork. The period under review for this information systems evaluation is \_\_\_\_\_ through \_\_\_\_\_.

**INSTRUCTION NOTE 4:** The questions must only be answered for all **financially significant information systems**. For the purposes of this questionnaire, financially significant information systems are defined as the computer hardware and software, including system programs and application programs, which are used to perform automated processing of a financially significant account balance or set of transactions. This includes financially significant e-business systems. Financially significant information systems are normally identified as "critical" in the insurance company's disaster recovery/business continuity plan.

**INSTRUCTION NOTE 5:** After the examiners have reviewed the company's narrative response to each question within each relevant section, along with the appropriate sample test documentation gathered by the company and available on the company premises, the examiners may determine that information systems controls appear to be in place at the company. If this is the case, it may be efficient for the examiners to test the information systems controls to determine whether the controls are operating effectively, thereby allowing the examiners to rely on the results of the control tests to reduce the level of substantive testing. Specific "test procedures" have been included throughout the questionnaire to help facilitate the nature and extent of the test procedures to be performed. In accordance with the control testing guidance contained in Part 3 of the *Financial Condition Examiners Handbook*, the control tests will consist of either judgmental sampling or attribute sampling. Some controls, such as information systems management controls, will be more subject to judgmental sampling, whereby the examiner inspects a judgmental number of information systems management reports issued during the period under review. Other controls, such as programming controls, will be more subject to attribute sampling, whereby the examiner would select as few as 11 program change documents, if the level of risk initially identified from the responses to the questionnaire was determined to be low and the level of intended reliance on the controls is low, or as many as 76 program change documents, if the level of risk initially identified from the responses to the questionnaire was determined to be high and the level of intended reliance on the controls is high.

**INSTRUCTION NOTE 6:** IS testing should be performed across all financially significant applications. Only one IS questionnaire may typically be completed by a company because many companies implement common controls across all applications. However, a company may not consistently apply and enforce the common controls across all applications. Some controls, such as inspection of the data center, are conducive to observation and are not subject to sampling. Other controls, such as programming and security authorization, are conducive to audit trail inspection and are subject to sampling. For those controls subject to sampling, the examiner should determine the appropriate sample size to be used based upon the level of inherent risk and the intended level of control risk applied against the compliance sample size table contained in Part 3 of the *Financial Condition Examiners Handbook*. For example, if the sample size is determined to be 70 and the company operates 7 financially significant applications within a common control infrastructure whereby only one IS questionnaire has been completed, the examiner should test 10 program changes for each application.

**SUMMARY OF SCOPING NOTES:**

Section A – No scoping note included, as completion of this section is required for all companies.

Section B – No scoping note included, as completion of this section is required for all companies.

Section C – This scoping note considers the conditions under which computer programs may undergo change.

Section D – This scoping note considers the conditions under which new computer systems may be developed and/or implemented.

Section E – No scoping note included, as completion of this section is required for all companies.

Section F– This scoping note considers whether the company has ever used or currently intends to use an outside computer processing service organization.

Section G – No scoping note included, as completion of this section is required for all companies

Section H – No scoping note included, as completion of this section is required for all companies.

Section I – This scoping note considers the status of current or planned e-commerce initiatives.

Section J – No scoping note included, as completion of this section is required for all companies.

**A. MANAGEMENT AND ORGANIZATIONAL CONTROLS**

**NOTE:** Management and Organization Control questions must be completed for each of the insurance company's financially significant organizational units that are directly responsible for maintenance or development, operation or security of financially significant production systems. Organization Control questions will typically be answered only once for centralized computer processing environments. In decentralized environments the questions may need to be answered more than once because separate organizational units may effectively have separate information systems departments.

The name, title and phone number of the insurance company's contact person responsible for providing the answers to this set of questions is:

---

**Guidance Point: Segregation of incompatible duties is an important element of the system of internal control. Appropriate segregation of duties helps to prevent mistakes, errors or potential fraud. Segregation of duties in smaller organizations may be difficult to achieve, because of a limited number of personnel. Compensating controls will be needed, such as assigning non-technical duties (e.g., data entry, input/reconciliation of control totals, etc.) to someone outside the data processing department. Likewise, strong data processing management and reporting controls, as well as proactive user involvement with the data processing function, may mitigate segregation of duties concerns.**

	Yes	No	Attachment
A1. Is there an IS steering committee or other evidence that top management is involved in the IS function and, if so, who are the members? Please provide copies of the steering committee meeting minutes or other evidence (e.g., memos or agendas) of steering committee meetings held during the period under review. <i>Test procedure: The examiner's evaluation of the minutes or other evidence provided, along with a judgmental sample of minutes or other evidence issued within the past 12 to 24 months, will generally be sufficient for this test.</i>			
A2. Is there an IS strategy consistent with the business strategy and, if so, has it been communicated by senior management to the rest of the individuals in the company? Please provide the table of contents or executive overview of the strategic plan for the business and information systems. <i>Test procedure: The examiner's evaluation of the table of contents or executive overview provided will generally be sufficient for this test.</i>			
A3. Is the IS department fully staffed and, if not, list the significant vacancies? Please provide an organization chart that identifies significant vacancies. <i>Test procedure: The examiner's evaluation of the chart provided will generally be sufficient for this test.</i>			
A4. Is the IS department independent of all operating units for which it performs data processing functions? Please provide evidence (e.g., from the organization chart) that data processing functions are independent from end user operating units. <i>Test procedure: The examiner's evaluation of the evidence provided will be sufficient for this test.</i>			

	Yes	No	Attachment
<p>A5. Are the IS roles and responsibilities clearly defined? Please provide a copy of a job function/description from each IS area (e.g., one from system maintenance and development, one from computer operations and one from computer security). <i>Test procedure: The examiner's evaluation of the job functions/descriptions provided will generally be sufficient for this test.</i></p>			
<p>A6. a. Are all incompatible functions, such as the initiation and authorization of transactions, or the custody of assets, performed outside the IS department? Please provide a copy of a description of the functions performed by the IS department. <i>Test procedure: The examiner's evaluation of the descriptions provided will be sufficient for this test.</i></p>			
<p>b. Are the functions of system design and programming adequately segregated from computer operations and data entry functions? Please provide a copy of these function descriptions. <i>Test procedure: The examiner's evaluation of the descriptions provided will generally be sufficient for this test.</i></p>			
<p>A7. a. Is there an internal audit function (internal or outsourced)?</p>			
<p>b. If so, is an IS division specialist on the staff?</p>			
<p>c. Are periodic tests or reviews of the system made by the internal or external audit staff to ensure that controls are functioning in accordance with established standards?</p> <p>Please provide the name and phone number of the audit contact person or senior IS specialist responsible for providing assistance to the IS examiners and a list of system reviews performed during the period under review over each financially significant system, along with copies of system review reports and/or test results. <i>Test procedure: The examiner's evaluation of the contact person's ability and availability to assist with the examination and the examiner's evaluation of the review documentation provided will generally be sufficient for this test.</i></p>			

**B. LOGICAL AND PHYSICAL SECURITY**

**NOTE 1:** Logical and Physical Security questions will typically be answered only once for centralized computer processing environments. In decentralized environments the questions may need to be answered more than once because separate organizational units may effectively have separate processing environments (i.e., each unit may have its own systems and local area networks).

**NOTE 2:** Virtually all insurance companies use some type of system-based logical security software in the mainframe environment or system-level security from the operating systems to restrict access to financially significant information systems. However, some insurance companies rely upon application-based security to restrict access to appropriate functions within financially significant applications while other insurance companies rely upon system-based security to secure both system access and application access. If the insurance company under examination relies upon system-based security to secure both system access and application access, questions B16 through B18 do **not** have to be answered.

The name, title and phone number of the insurance company’s contact person responsible for providing the answers to this set of questions is:

**Guidance Point:** Well controlled companies have reporting mechanisms in place that allow management to monitor both authorized and unauthorized attempts to access sensitive computer facilities. These reports are reviewed regularly by security administration personnel. Persistent attempts by individuals to gain unauthorized access to these facilities are reported to senior data processing management. Additionally, access by individuals to these facilities that appears inappropriate is investigated to determine whether it is consistent with the individual’s job responsibilities.

B1. Does management demonstrate an awareness of security risks, recognize that security is both a technical and operational, as well as a cultural issue, and promote security awareness across all levels of the organization? Please provide a copy of the company security policy and evidence of security awareness training. *Test procedure: The examiner’s evaluation of the material provided.*

**Guidance Point:** The security administrator’s role is to ensure that only appropriately authorized individuals are granted access to system and application resources. The security officer’s role is responsible for the monitoring, modification, and enforcement of the access control strategy, as well as the overall security strategy for the organization. The security function should be positioned within the company’s structure in a location that enables it to be an adequate control function. It should be segregated from other departments that may affect its objectivity. Security can be accomplished successfully from either a centralized or decentralized location. Although neither approach is better than the other, the type selected must fit the company’s structure. If the company is relatively small to medium in size, it may not have both a full-time security administrator and security officer.

Yes	No	Attachment

	Yes	No	Attachment
B2. Does the company's information security policy clearly define the responsibilities of users, management and security personnel? <i>Test procedure: The examiner's evaluation of the policy provided will generally be sufficient for this test.</i>			
B3. Are the assigned tasks of the individual responsible for information security consistent with the company's security policy statement? Please provide a list of all personnel with security administration responsibilities. <i>Test procedure: The examiner's evaluation of the information provided will generally be sufficient for this test.</i>			

**Guidance Point: Well-controlled companies restrict physical access to sensitive computer/communication facilities (e.g., the computer room and the network operations center) using many methods, which include: smart cards, combination numbers and keys. These control procedures operate at all times, including evenings, weekends, and holidays.**

**PHYSICAL SECURITY**

	Yes	No	Attachment
B4. a. Are there physical access controls over the computer/communication facilities, such as, wiring closets, server rooms, etc, including:			
b. Are the computer/communication facilities located out of the main flow of traffic away from public view?			
c. Are the computer/communication facilities behind substantial walls?			
d. Do the computer/communication facilities have a fire detection system and/or a fire suppression system, such as sprinklers charged with water at points outside the computer room?			
e. Are computer/communication facilities protected from damage resulting from electronic power interruption, surges and spikes? Please provide the name and phone number of the person who can arrange a tour of the computer/communication facilities. <i>Test procedure: The examiner's observation of the data center will generally be sufficient for this test.</i>			
B5. Has a written statement been issued that defines the restrictions on access to the computer/communication facilities? Please provide a copy of the statement. <i>Test procedure: The examiner's evaluation of the written statement provided will generally be sufficient for this test.</i>			
B6. a. Are procedures in effect in the computer/communication facilities to verify that only authorized individuals are being permitted to enter the facility? Please provide a copy of the procedures and the name and phone number of the person who can demonstrate or validate the procedures. <i>Test procedure: The examiner's evaluation of the procedures provided, corroborating inquiry with the person identified, and observation of the procedures, if possible, will generally be sufficient for this test.</i>			



	Yes	No	Attachment
<p>f. Does the system automatically prompt users to change their passwords at least quarterly and prevent passwords from being reused by the same individual? Please provide a printout of the security parameters, such as password aging and password history.</p>			
<p>B9. Are system/resource/internet security authorization forms completed and approved by management to ensure that system and internet access granted to users and IS staff is commensurate with their job responsibilities? Please provide a list of all authorized system users, including system or application account IDs, for each platform on which financially significant applications reside. If one platform (e.g., Windows or Novell) is used to authenticate all users to the company network, then one list will be sufficient, so long as all users from all significant computer systems are included on this list. <i>Test procedure: The examiner should select an attribute sample of users from the list provided by the company. If all financially significant information systems reside on the same computer platform or essentially similar computer platforms that are subject to the same or similar logical security controls, it is sensible to select a single attribute sample. If not, an attribute sample should be selected from the population of employees who have security access accounts on each dissimilar computer platform.</i></p>			
<p>B10. Does user department management periodically validate the access capabilities currently provided to individuals in their department? Please provide evidence of the last user access review performed during the period under review. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i></p>			
<p>B11. Do procedures provide for prompt cancellation of identification codes and passwords when the employment of the individual to whom they were assigned has been terminated? Please provide a copy of the procedures and evidence that the procedures were followed for the last IS person or user terminated, if any, during the period under review. <i>Test procedure: The examiner's evaluation of the procedures and evidence provided will generally be sufficient for this test.</i></p>			
<p><b><u>Guidance Point: Well-controlled companies have reporting mechanisms in place to monitor security events (e.g., invalid logon attempts, unauthorized attempts to access data and programs, changes to software security values and rules). These reports are reviewed regularly by security personnel. Persistent attempts by individuals to gain unauthorized access to resources are reported to the applicable application owners (e.g., the manager of the claims department) and/or senior management</u></b></p>			
<p>B12. Does management review and resolve reports of security violations? Please provide evidence of IS management's review of security violation reports and subsequent resolution of violations. <i>Test procedure: the examiner's evaluation of the evidence provided will generally be sufficient for this test.</i></p>			

B13. Do procedures exist which require authorized users of computing resources to be given specific permission to access particular resources, including data files, applications, the operating system and utilities? Please provide a copy of the procedures. *Test procedure: The examiner's evaluation of the procedures provided will generally be sufficient for this test.*

B14. Is there a control that ensures appropriate restriction of remote access (e.g., through networks or using dial-up facilities)? Please provide a summary or list of all methods of remote access. Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. *Test procedure: The examiner's evaluation of the control, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.*

**Guidance Point: Well-controlled companies periodically verify that access to application resources is appropriate. Typically, this is accomplished by distributing lists of the individuals with access privileges to application functions and features, program libraries and data files to application owners and data processing management to confirm that such access is appropriate.**

B15. Is there a control that ensures that users are restricted to their applications (i.e., preventing users from escaping from application menus)? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. *Test procedure: The examiner's evaluation of the control, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.*

B16. Is there an application level control that ensures the effectiveness of financially significant application password controls (e.g., unique user IDs and passwords)? Please provide a copy of the logical security procedures used to determine the structure and use of application passwords (e.g., password expiration and password confidentiality) and the name and number of the person who can demonstrate or validate the procedures. *Test procedure: The examiner's evaluation of the procedures, corroborating inquiry with the person identified and observation of the procedures, if possible, will generally be sufficient for this test.*

B17. a. Are application security authorization forms completed and approved by management to ensure application access granted to users is commensurate with their job responsibilities? Please provide a copy of a completed and approved application security authorization form for one user from each financially significant application. *Test procedure: The examiner's evaluation of the application security authorization forms provided, along with the application security authorization forms on file for the employees selected from the attribute sample selected for question B9 above, should be sufficient for this test.*

Yes	No	Attachment

	Yes	No	Attachment
<p>b. Are periodic checks carried out to confirm that employees' current <u>application</u> access is commensurate with their job responsibilities? Please provide evidence of the last check performed during the period under review. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i></p>			
<p>B18. Are there procedures that ensure that <u>application</u> access is appropriately changed on a timely basis when employees transfer or terminate? Please provide a copy of the procedures and evidence that the procedures were followed for the last user terminated, if any, during the period under review. <i>Test procedure: The examiner's evaluation of the procedures and related evidence will generally be sufficient for this test.</i></p>			
<p>B19. a. Is there an appropriate sign-out procedure for computer equipment that is removed from the company's offices?</p>			
<p>b. Does the equipment have asset management tags affixed and recorded in an asset management system?</p>			
<p>Please provide a copy of the procedure and the name and phone number of the person who can demonstrate and validate the procedure. <i>Test procedure: The examiner's evaluation of the procedure, corroborating inquiry with the person identified, and observation of the procedure, if possible, will generally be sufficient for this test.</i></p>			
<p><b><u>Guidance Point:</u> In responding to unusual circumstances it may be necessary to bypass some of the security protection. A policy for dealing with such emergencies should be prepared. Activities during the emergency should be logged carefully. Once the emergency is over, security protection should be reinstated immediately. The impact of the activities during the emergency should be assessed and authorized retrospectively, and appropriate corrective action should be taken. Emergencies during the day can be corrected by a responsible technical support person with a user-ID with special privileges. If a problem occurs outside of normal working hours, the off-shift personnel (e.g., on-call programmer) may need a special user ID.</b></p>			
<p>B20. Is there a control over administrator-level access to the operating system that ensures access to sensitive software utilities is appropriately restricted and monitored (consider the use of these sensitive facilities during an emergency situation)? Please provide a list of the sensitive software utilities commonly used by the company and evidence that the last use of each utility during the period under review was approved.</p>			
<p>B21. If applicable, are personnel with access to sensitive software utilities restricted access to physical financially significant assets? Please provide a copy of the job description for the last person who executed each of the utilities identified in question B20. <i>Test procedure: The examiner's evaluation of the job description provided will generally be sufficient for this test.</i></p>			

**Guidance Point:** Such procedures typically include notifying management, including the legal and public relations departments. These procedures may also include guidelines for contacting law enforcement at the discretion of senior corporate management.

B22. Does the company have formal emergency response procedures to follow if a computer security incident occurs? Please provide a copy of the incident response procedure. *Test procedure: The examiner's evaluation of the procedures will generally be sufficient for this test.*

B23. Does the company have formal monitoring procedures and systems to detect unauthorized access attempts from either outside or inside the company? Please provide copies of the intrusion detection policy, documentation of the systems in place and the review process followed. Please provide the name and phone number of the person who can provide evidence of the use of intrusion detection systems and/or penetration studies. *Test procedure: The examiner's review of the documentation and corroborating inquiry with the person identified and observation of the technology in use will be sufficient evidence for this test.*

B24. a. Has management developed a comprehensive policy addressing the unique security risks associated with wireless technologies? Please provide a copy of policies addressing wireless technology risks.

b. Does the company monitor for rogue access points? Please provide evidence of the most recent scan for rogue access points. *Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for these tests.*

B25. Does the company utilize a virus detection system on all personal processing devices (desktops workstations, laptops, notebooks, personal information devices (PIDs), etc.) that are regularly updated and, if yes, does it have a disinfecting feature (i.e., the ability to restore files to a healthy state)?

Where remote access is permitted, are remote devices scanned for current versions of the virus-scanning engine and the virus definition library prior to the network?

Please provide the name of the virus detection and/or anti-virus software, the company's methodology for distributing and updating the software, and the name and phone number of the person who can provide evidence of the mandatory, periodic use and update of the anti-virus software across the network. *Test procedure: The examiner's corroborating inquiry with the person identified and observation of the software in use will generally be sufficient for this test.*

Yes	No	Attachment



**C. CHANGES TO APPLICATIONS**

**NOTE:** Changes to Applications questions must be completed for financially significant production applications, both internally developed and purchased packages, which were changed during the period under review.

The name, title and phone number of the insurance company's contact person responsible for providing the answers to this set of questions is:

	Yes	No	Attachment
<p>C1. Does management monitor the level of open requests for changes to applications and the satisfaction of users with changes made? Please provide a copy of reports on application performance, which have been reviewed and approved by management and include information regarding the volume of changes made to applications, application problems, emergency fixes, application related help desk calls, backlog of requests from users for application changes and users' views on the functional and operational quality of applications. <i>Test procedure: The examiner's evaluation of the reports and evidence provided will generally be sufficient for this test.</i></p>			
<p>C2. Is there a control that ensures that user needs result in appropriate program change requests and the requests are properly evaluated, prioritized, authorized, monitored and tested? Please provide a list of all program change requests made during the period under review. <i>Test procedure: The examiner's evaluation of the list of program changes and the related evidence provided, along with an attribute sample of between 11 and 76 program changes made within the past 12 to 24 months on each computer processing platform that contains a financially significant information system, will generally be sufficient for this test. Items that should be considered by the examiner include: (1) evidence of cost justification for the most significant program change from each system, evidence of user and IS management written authorization of the most significant change from each system; (2) evidence of user and IS management review and approval of each of the most significant program changes completed for each system; (3) evidence that management reviewed the test plans to see that the level of testing was appropriate for the risk involved in the application change; and (4) evidence that management reviewed the final test results. If all financially significant information systems reside on the same computer platform or essentially similar computer platforms that are subject to the same or similar program change controls, it is sensible to select a single attribute sample from the population of program changes made on these platforms. However, if financially significant information systems reside on separate or essentially dissimilar computer platforms that are not subject to the same or similar program change controls, an attribute sample should be selected from each computer platform</i></p>			

	Yes	No	Attachment
C3. a. Is there a control that ensures that the correct program libraries are updated with the most recent version of the program? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: The examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i>			
b. Is there a control that ensures that the source code used corresponds to the most recent version of the program and modifications to a program by more than one programmer are coordinated? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: the examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i>			
C4. a. Is there a control that would prevent or detect unauthorized changes made after the completion of testing but before transfer to the live environment? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: the examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i>			
b. Is there a control that ensures that only properly tested, reviewed and approved changes are transferred into the production environment? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: the examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i>			
C5. Where applications run at multiple sites, is there a control that ensures that all copies of production programs are updated? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: the examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i>			
C6. Is application documentation appropriately updated and distributed to affected users and IS staff? Please provide a copy of updated application documentation for the most significant program change made from question C2. <i>Test procedure: the examiner's evaluation of the individual attachments provided will generally be sufficient for this test.</i>			
C7. Is technical documentation updated to reflect program or database structural changes? Please provide a copy of updated technical documentation for the most significant program and/or database changes made from question C2. <i>Test procedure: the examiner's evaluation of the individual attachments provided will generally be sufficient for this test.</i>			



**D. SYSTEM AND PROGRAM DEVELOPMENT**

**NOTE:** System and Program Development questions must be completed for new financially significant production applications that were developed in-house during the period under review or purchased and modified during the period under review.

To the extent new System and Program Development (Section D) and Changes to Applications (Section C) follow the same processes, responses to certain questions may be referenced to answers within Section C.

The name, title and phone number of the insurance company’s contact person responsible for providing the answers to this set of questions is:

	Yes	No	Attachment
<p>D1. Is there a control that ensures that all necessary steps are appropriately included in a project plan (e.g., use of a system development methodology)? Please provide a copy of an overview of the current system development life cycle methodology (SDLC) and a copy of the policy that requires development projects to have a clear sponsor at the senior management level. <i>Test procedure: The examiner’s evaluation of the documentation provided will generally be sufficient for this test.</i></p>			
<p>D2. Do user departments (e.g., accounting department), auditors (e.g., external and internal), computer operation and system architect personnel participate in the early stages of planning and development of new systems? Please provide evidence of user department, auditor and computer operations involvement throughout each significant project identified in question D3 (e.g., documented attendance at project review meetings and/or memo's documenting involvement). <i>Test procedure: The examiner’s evaluation of the evidence provided will generally be sufficient for this test.</i></p>			
<p><b><u>Guidance Point:</u> A well-controlled company performs feasibility studies, including cost benefit analyses, to determine the effects on existing hardware (e.g., processing and storage capacity) and system software of new or significantly enhanced applications. These studies also determine whether the existing hardware and system software configuration is compatible with the application. For example, a company may use an IBM mainframe computer to process their financial applications; however, they are considering the purchase of financial application software that was designed to be processed using a HP computer.</b></p>			
<p>D3. Do plans include cost justification? Please provide a list of projects during the period under review and a copy of a project cost justification for the most significant project from each system (i.e., most significant in terms of cost or business impact). <i>Test procedure: The examiner’s evaluation of the individual attachments provided will generally be sufficient for this test.</i></p>			
<p>D4. Does senior management approve the plan before work commences? Please provide evidence of senior management approval of the project plan for the most significant projects identified in question D3. <i>Test procedure: The examiner’s evaluation of the evidence provided will generally be sufficient for this test.</i></p>			

**Guidance Point: In any new or significantly enhanced application, some desired features are likely to be overlooked during the initial stages of design and development. As these features are identified, modifications to the initial specifications should be documented and subject to the same request, feasibility and design procedures as the initial application.**

- D5. Is there a procedure that provides for management’s review of progress on the project at critical stages of its development and, if so, does the procedure provide that work cannot progress to the next phase (systems design, programming, testing, conversion, etc.) until and unless approval has been given? Please provide evidence of senior management’s review of progress for each significant project identified in question D3. *Test procedure: The examiner’s evaluation of the evidence provided will generally be sufficient for this test.*
- D6. Is there a systems design standards manual? Please provide a copy of the index from the manual. *Test procedure: The examiner’s evaluation of the index provided will generally be sufficient for this test.*
- D7. Is there a programming standards manual? Please provide a copy of the index from the manual. *Test procedure: The examiner’s evaluation of the index provided will generally be sufficient for this test.*

**Guidance Point: A well-controlled company has policies that require test plans to be developed for new or significantly enhanced applications. The planning documentation should include tests to be performed, expected results and how test data will be developed. Normally, the test plan is reviewed and approved by the application owners and data processing management. Depending on the complexity of the application, the level and extent of testing may vary. For example, when a single application is implemented, such as payroll, testing would normally be performed to ensure programs work individually and in conjunction with each other, and interface appropriately with existing applications. In a highly integrated application, such as claims processing, testing would tend to cover the areas noted above, as well as between specific subsystems, such as the general ledger.**

- D8. Is there a control that prevents testing from being performed on production data files? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. *Test procedure: The examiner’s evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.*
- D9. Is appropriate program testing performed by the IS staff, QA staff and users to prevent or detect errors in program coding and ensure that the application operates as intended in the production environment and provides appropriate data output? Please provide evidence of program test results for each major project identified in question D3. *Test procedure: The examiner’s evaluation of the evidence provided will generally be sufficient for this test.*

Yes	No	Attachment

	Yes	No	Attachment
D10. Is there a control that ensures that when modifications are made subsequent to initial testing they are also subject to appropriate program testing procedures? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: The examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i>			
D11. Is there a control that ensures that unauthorized changes cannot be made after the completion of program testing but before transfer into the production environment? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: The examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i>			
D12. Is an effort made to perform a parallel run by program and by system, where possible? Please provide for each project identified in question D3, evidence of parallel test results, if any, including evidence of management's review. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i>			
D13. Is there a control that ensures that purchased software packages are subject to adequate selection procedures, such as a thorough investigation of package capabilities compared to business needs and system architecture and a thorough comparison of several packages to one another? Please provide a list of financially significant software packages that were purchased during the period under review and evidence of management's justification for each purchase. <i>Test procedure: The examiner's evaluation of the list and evidence provided will generally be sufficient for this test.</i>			
<b><u>Guidance Point:</u> Vendor application software generally provides options that allow the user, to some extent, to customize the application for their unique purposes. These options are often called parameters, and, for example, can be used to alter aging categories, prepare customized trial balances, or modify the selection criteria for reporting.</b>			
D14. Is there a control that ensures that packaged software options selected and parameters set are appropriate to achieve business and application control requirements? Please provide evidence of management's review of options selected and parameters set for each project identified in question D3. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i>			
D15. Does the company have legal ownership or rights (e.g., escrow account) to the application source code for software?			
D16. Is the conversion process controlled for old transaction data, standing data and establishment of data not used by the old application? Please provide evidence of management's review and approval of the data conversion plan and data conversion results for each major project identified in question D3. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i>			

	Yes	No	Attachment
D17. Is user documentation available to users at implementation? Please provide a copy of the index to user documentation manuals prepared as part of the most significant project identified in question D3. <i>Test procedure: The examiner's evaluation of the index will generally be sufficient for this test.</i>			
D18. Is the technical documentation available to technical staff at implementation? Please provide a copy of the index to technical documentation manuals prepared as part of the most significant project identified in question D3. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i>			
D19. Is program code secured for access by only authorized individuals? Please describe procedures to secure directories, datasets or other containers of source code, code being tested, tested code awaiting movement to production areas, and production object code for financially significant systems. <i>Test procedure: The examiner's evaluation of the list provided, corroborating inquiry with the person identified and observation of the storage areas, if practical, will generally be sufficient for this test.</i>			
D20. Has the company issued written policy statements regarding the user development of financially significant applications and/or tools and reports? If yes, do the statements include appropriate requirements for development and testing, documentation, input, processing and output controls, backup and recovery of programs and data and security over custody and use of personal computer assets, including hardware, software and data? Please provide copies of the policy statements. <i>Test procedure: The examiner's evaluation of the statements provided will generally be sufficient for this test.</i>			

## E. CONTINGENCY PLANNING

The name, title and phone number of the insurance company's contact person responsible for providing the answers to this set of questions is:

	Yes	No	Attachment
E1. Is the disaster recovery/business contingency plan:			
a. current;			
b. based on a business impact analysis;			
c. tested periodically; and			
d. developed to address all significant business activities, including financial functions, telecommunication services, data processing and network services? Please provide a copy of the plan and evidence of test results, including management's resolution of test discrepancies. <i>Test procedure: The examiner's evaluation of the plan and evidence provided will generally be sufficient for this test.</i>			
E2. a. Does the disaster recovery/business continuity plan clearly describe senior management's roles and responsibilities associated with the declaration of an emergency and implementation of the disaster recovery/business continuity and disaster recovery plans			
b. Does the plan clearly identify the general process by which the threat will be assessed and the specific individuals who are authorized to declare an emergency?			
c. Does the plan address communication of the disaster event and provide for alternative points of contact (if necessary) to customers, vendors and state and other regulatory officials?			
Please indicate where individuals with the authority to declare an emergency are listed within the plan document. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i>			
E3. a. Does the plan contain a list of critical computer application programs, operating systems and data files?			
b. Does the plan contain a list of the supplies that would be needed in the event of a disaster, together with names and phone numbers of the suppliers?			
Please provide same as question E1. <i>Test procedure: Same as question E1.</i>			
E4. Has a restoration priority been assigned to all significant business activities? Please provide a copy of the prioritized business activities. <i>Test procedure: The examiner's evaluation of the activities provided will generally be sufficient for this test.</i>			
E5. Have user departments developed adequate manual processing procedures for use until the electronic data processing function can be restored? Please provide the name and phone number of one person from each financially significant user area who can demonstrate the procedures. <i>Test procedure: The examiner's corroborating inquiry with the people identified and observation of the procedures, if possible, will generally be sufficient for this test.</i>			

- E6. Are copies of the plan kept in relevant off-site locations? Please provide a list of the locations and the name and phone number of the person who can validate the existence of the copies at the off-site locations. *Test procedure: The examiner's evaluation of the list and corroborating inquiry with the person identified will generally be sufficient for this test.*
- E7. Are current backup copies of programs, essential documents, records and files stored in an off-premises location? Please provide an inventory of the contents of off-premises locations and the name and phone number of the person who can be contacted to verify the contents of the off-premises locations. *Test procedure: The examiner's evaluation of the inventory list and corroborating inquiry with the person identified will generally be sufficient for this test.*
- E8. Does a written agreement or contract exist for use by IS of a specific alternate site and computer hardware to restore data processing operations after a disaster occurs and does the site have a backup generator in place in case of local power outages, a fire detection and suppression system and moisture sensors in place under the raised floor? Please provide a copy of the agreement and the name and phone number of the person who can validate the existence of the equipment at the alternate site. *Test procedure: The examiner's evaluation of the agreement and corroborating inquiry with the person identified will generally be sufficient for this test.*

Yes	No	Attachment

**Scoping Note – Section F**

Does the company use any service organizations for any processing, development or system management? (This section should be completed even if the entire information system process is completed by a service organization. However, if this is the case, the other components of this exhibit should be completed by the service organization.)

*A service organization is considered any affiliate or non-affiliate providing processing, development or system management.*

YES	NO

If the answer to the above question is YES, the company’s respective IS manager should complete Section F of the questionnaire. If the answer is NO, the company’s respective IS manager should not complete Section F of the questionnaire, but should describe below, or in an attachment, whether the company has ever used or currently intends to use an outside computer processing service organization. This information will be evaluated by the examiner to confirm whether or not any part of this section should be completed and tested.

---

---

---

---

---

---

---

---

---

---

**F. SERVICE PROVIDER CONTROLS**

**Note:** The company should complete a separate Service Provider Questionnaire (Attachment B) for each organization providing services described in the scoping note. In addition, the following questions must be answered. If the answers are uniform for all service provider contracts, the questions may be answered here. If the answers are different by service provider contract, provide an attachment answering the questions to each completed Service Provider Questionnaire.

The name, title and phone number of the insurance company’s contact person responsible for providing the answers to this set of questions is:

---

	Yes	No	Attachment
F1. Does the insurance company carry insurance of its own to compensate for losses caused by the service provider? Please provide a copy of the insurance company’s policy covering potential losses caused by the service provider. <i>Test procedure: the examiner’s evaluation of the insurance policy will generally be sufficient for this test.</i>			
F2. Is the insurance company the legal owner of all programs as well as tapes, disks, documentation, etc., used in the processing of its applications and is the insurance company the legal owner of data records created exclusively for the insurance company and/or the company’s affiliate(s)? Please provide a list of any exceptions. <i>Test procedure: The examiner’s evaluation of the documentation provided in Attachment B will generally be sufficient for this test.</i>			
F3. Can any service provider legally confiscate the insurance company’s data, data recording media, or programs? Please provide a list of the service providers with this capability. <i>Test procedure: The examiner’s evaluation of the documentation provided in Attachment B will generally be sufficient for this test.</i>			

## G. OPERATIONS

**NOTE:** Operations questions will typically be answered only once for centralized computer processing environments. In decentralized environments, the questions may need to be answered more than once because separate organizational units may effectively have separate operations environments.

The name, title and phone number of the insurance company's contact person responsible for providing the answers to this set of questions is:

	Yes	No	Attachment
<p>G1. Is an inventory of hardware and software maintained? Please provide an inventory of hardware and software on the spreadsheet provided (Attachment A).</p>			
<p>G2. a. Does management make use of automated tools to record mainframe, server and network performance and use the output of these tools to proactively upgrade or replace components when they approach their operating capacity or show signs of imminent failure? Please provide the name and phone number of the person(s) who can confirm the use of mainframe, server and network monitoring tools.</p>			
<p>b. Does IS management provide a periodic maintenance schedule for changes to computer systems and infrastructure as well as a mechanism by which the ramifications of these changes can be considered by all impacted groups? Please provide a log of all significant systems and infrastructure changes implemented during the last year of the period under review, including evidence of the review of these changes by impacted groups. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i></p>			
<p>G3. Is there a control that ensures the prior release of a program can be restored if an upgrade causes a problem in the production environment? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control. <i>Test procedure: The examiner's evaluation of the control description, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i></p>			
<p>G4. Is there a standard operations procedures manual that is current and enforced? Please provide a copy of the index from the manual. <i>Test procedure: The examiner's evaluation of the index will generally be sufficient for this test.</i></p>			
<p>G5. Is there a control that ensures that all changes to preapproved job schedules are appropriate and authorized? Please provide a description of the control and evidence of management's approval of the last job schedule change made during the period under review. <i>Test procedure: The examiner's evaluation of the control and evidence provided will generally be sufficient for this test.</i></p>			

	Yes	No	Attachment
G6. Are on-site backup copies of data files and programs maintained in a locked waterproof and fireproof storage area? Please provide an inventory of the contents of the storage area and the name and phone number of the person who can arrange a tour of the storage area. <i>Test procedure: The examiner's evaluation of the inventory, corroborating inquiry with the person identified and observation of the storage area, if practical, will generally be sufficient for this test.</i>			
G7. a. Is a records-retention program in effect to define how long data and backups must be retained? Please provide a copy of record-retention policies and procedures, the considerations used in devising the policy and procedures and an assessment of whether they are in compliance with applicable regulatory requirements.			
b. Does the program include data generated through e-commerce? Please provide a copy of the e-commerce electronic record keeping policy and the contact information for a person responsible for ensuring compliance with this policy.			
c. Does the program address scanned image documents? <i>Test procedure: The examiner's evaluation and assessment of the policies and procedures will generally be sufficient for this test.</i>			
<b><u>Guidance Point: Operational failures can include network failures. This guidance point applies to Questions G8 through G9.</u></b>			
G8. a. Are there appropriate escalation procedures in place to report and resolve operational failures in a timely manner?			
b. Are appropriate IS staff and, where appropriate, users involved in the resolution of operational failures? Please provide a copy of the escalation procedures and evidence of compliance with the escalation procedures during the last operational failure. <i>Test procedure: The examiner's evaluation of the escalation procedures and evidence of compliance during the latest failure or major processing disruption along with a judgmental sample of evidence selected over the past 12 to 24 months will generally be sufficient for this test.</i>			
G9. Is there a control that ensures that the underlying causes of operational failures are identified and addressed (as opposed to applying short-term fixes)? <i>Test procedure: The examiner's evaluation of the evidence provided, along with a judgmental sample of evidence selected over the past 12 to 24 months, will generally be sufficient for this test.</i>			
G10. Is there a control that ensures the effective administration of databases including integrity checks (e.g., is it the responsibility of a database administrator)? Please provide a job description for the database administrator and the name and phone number of the administrator. <i>Test procedure: The examiner's evaluation of the job description and corroborating inquiry with the person identified will generally be sufficient for this test.</i>			
G11. Does insurance coverage exist to protect against loss of equipment, programs and data? Please provide a copy of the insurance policy. <i>Test procedure: The examiner's evaluation of the coverage provided for in the insurance policy will generally be sufficient for this test.</i>			

	Yes	No	Attachment
G12. If the company provides data processing services for others, is there insurance to protect it from liability for errors and omissions? Please provide a copy of the insurance policy. <i>Test procedure: the examiner's evaluation of the coverage provided for in the insurance policy will generally be sufficient for this test.</i>			
G13. Are system updates (patches, anti-virus/anti-malware, etc) monitored to ensure that all systems are updated in a timely manner? Please provide a description of the technology used to keep systems current (e.g., Windows server update service). If a manual approach is used to maintain system updates, please provide a description of the manual procedures. <i>Test procedure: The examiner's evaluation of the evidence provided will generally be sufficient for this test.</i>			
<b><u>Guidance Point:</u> System software is the computer programs and related procedures that control the processing of the computer hardware and non-application-related functions. Examples of system software include the operating system, security software, tape management system, job scheduling software, telecommunications and network software, and the underlying database management software.</b>			
G14. Is the selection of system hardware and software and related options controlled? Please provide a copy of system hardware and software selection and option review procedures. <i>Test procedure: The examiner's evaluation of the procedures provided will generally be sufficient for this test.</i>			
G15. Are new systems or upgrades to existing system hardware or software appropriately tested before being moved to the production environment? Please provide a description of the control, a list of all system hardware or software changes made during the period under review, and a copy of the most significant change, including test results and IS management approval. <i>Test procedure: The examiner's evaluation of the control and list provided, test results and evidence of management's approval provided, along with the same information for a judgmental sample of system software changes made over the past 12 to 24 months, will generally be sufficient for this test.</i>			
G16. Is the process used in changing the system architecture documented? Please provide a copy of the documented process and the name and phone number of the person who can demonstrate or validate the process. <i>Test procedure: The examiner's evaluation of the process, corroborating inquiry with the person identified and observation of the process, if possible, will generally be sufficient for this test.</i>			
<b>NOTE: Questions G17-G21 relate primarily to Mainframe Computers</b>			
G17. Does batch-scheduling software allow for the creation of triggers and dependencies that start, stop, or pause batch cycles based on the availability of resources and data and the successful completion of prerequisite jobs? Please provide a description of the batch scheduling controls and the name and phone number of the person who can demonstrate or validate the function.			

*Test procedure: the examiner's evaluation of the function, corroborating inquiry with the person identified and observation of the function, if possible, will generally be sufficient for this test.*

G18. Is the execution of jobs logged or otherwise documented and, if so, is the ability to alter the log controlled? *Test procedure: The examiner should review and evaluate a sample of logs produced and determine what logical and/or physical security measures protect them.*

G19. Is machine operation activity captured on the system and is there an independent reporting and examination of machine activity to check operator performance and machine efficiency and, if so, by whom? Please provide for the period under review, evidence of the latest IS review of operation activity or error reports and subsequent investigation and resolution of operation problems. *Test procedure: The examiner's evaluation of the evidence provided, including evidence of the subsequent investigation and resolution of the problems, will generally be sufficient for this test.*

G20. Are internal file labels used on all magnetic tape files? Please provide the name and phone number of the person who can demonstrate or validate the use of internal file labels. *Test procedure: The examiner's corroborating inquiry with the person identified and observation of the use of internal file labels, if possible, will generally be sufficient for this test.*

G21. Are console operators permitted to override operating system label error messages (such as unexpired file) and, if so, under what circumstances? Please provide a description of the circumstances and the name and phone number of the person who can demonstrate or validate the circumstances. *Test procedure: The examiner's evaluation of the circumstances, corroborating inquiry with the person identified and observation of the circumstances, if possible, will generally be sufficient for this test.*

Yes	No	Attachment

## H. PROCESSING CONTROLS

The name, title and phone number of the insurance company's contact person responsible for providing the answers to this set of questions is:

	Yes	No	Attachment
<p>H1. Are there control procedures in place to ensure electronic data transmissions are transmitted and received completely and accurately? Please provide a copy of the control procedures and the name and phone number of the person who can demonstrate or validate the procedures. <i>Test procedure: The examiner's evaluation of the control, corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i></p>			
<p>H2. Are there control procedures in place to detect data that is input inaccurately or incompletely? Please provide a description of the control and the name and phone number of the people who can demonstrate or validate the control for each financially significant application. <i>Test procedure: The examiner's evaluation of the control, corroborating inquiry with the people identified and observation of the control, if possible, will generally be sufficient for this test.</i></p>			
<p>H3. If there are any negotiable forms, such as checks, are they kept under strict inventory control? Please provide the name and phone number of the person who can demonstrate or validate inventory control. <i>Test procedure: The examiner's corroborating inquiry with the person identified and observation of the control, if possible, will generally be sufficient for this test.</i></p>			
<p>H4. Does the audit trail of records and reference provide the means to adequately trace any transaction forward to the final total, trace any transaction back to the original source document or input and trace any final total back to the component transactions? Please provide audit trail documentation for one transaction from each financially significant application. <i>Test procedure: The examiner's evaluation of the audit trail for the transaction provided from each financially significant application, as well as a judgmental test of at least one more transaction for each financially significant application, will generally be sufficient for this test.</i></p>			
<p>H5. Does the company have a data warehouse which includes financially significant data? If so, identify the types of data which are accumulated in the data warehouse and the document the process for ensuring that the data warehouse accurately and completely represents the data in the company's production systems. <i>Test procedure: The examiner's identification of the data accumulated in the data warehouse and review and observation of the controls over reconciliation of the information transferred to the data warehouse will generally be sufficient for this test.</i></p>			

**Scoping Note – Section I**

NOTE: The company should describe the status of current or planned e-commerce initiatives. E-commerce methods of transmission may include voice recognition units (VRUs), the Internet, third-party extranets and wireless and broadband communications media.

Does the company utilize e-commerce for the submission, acceptance and/or changes to policies?

Does the company utilize e-commerce for the submission, acceptance and/or the processing of claims and/or annuity products?

Does the company utilize e-commerce in the processing, or to supplement the processing of any other financially significant account balances or sets of transactions described in Instruction Note 4, such as investments, reinsurance, procurement, employee benefits, etc.?

**NOTE:** If the answer to ANY of the above questions is YES the company should complete section I. If the answer to ALL questions is NO, the company should not complete section I of the questionnaire.

	Yes	No
Does the company utilize e-commerce for the submission, acceptance and/or changes to policies?		
Does the company utilize e-commerce for the submission, acceptance and/or the processing of claims and/or annuity products?		
Does the company utilize e-commerce in the processing, or to supplement the processing of any other financially significant account balances or sets of transactions described in Instruction Note 4, such as investments, reinsurance, procurement, employee benefits, etc.?		

## I. E-COMMERCE CONTROLS

The name, title and phone number of the insurance company's contact person responsible for providing the answers to this set of questions is:

	Yes	No	Attachment
<p>11. Are the company's e-commerce initiatives led by a knowledgeable team including executive management and IS security personnel? Please provide the organizational chart for e-commerce initiatives and the job descriptions and resumes for key e-commerce leaders. <i>Test procedure: The examiner's evaluation of the e-commerce organization chart, job descriptions and resumes will generally be sufficient for this test.</i></p>			
<p><b><u>Guidance Point:</u> The c-commerce strategy should be closely linked to the overall corporate strategy. Personnel documentation could include a mapping of the required skill set to the current employee skill set inventory, a document outlining the company's criteria for outsourcing or hiring personnel with requisite skills or a description of the company's E-Commerce training program.</b></p>			
<p>12. a. Is a formal e-commerce strategy included in the company's strategic plan and?</p>			
<p>b. Does the strategy include consideration of the availability of appropriate technology, as well as technically competent personnel, necessary to support the company's e-commerce initiatives?</p> <p>Please provide a copy of the strategy. <i>Test procedure: the examiner's evaluation of the strategy document will generally be sufficient for this test.</i></p>			
<p>13. Has company management developed a formal document that clearly defines the tactical methods and technologies for implementing the company's e-commerce strategy? Please provide a copy of this document. <i>Test procedure: The examiner's evaluation of the implementation document (typically a tactical or project plan) explaining how the e-commerce strategy should be executed will generally be sufficient for this test.</i></p>			
<p><b><u>Guidance Point:</u> The responsibility for monitoring pending regulations and compliance with new regulations should be formally assigned, typically to a compliance function or a risk management function. Consider whether the company has assigned responsibility for relevant regulations, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPPA), the Electronic Signature in Global and National Commerce Act (E-SIGN), and the European Union Safe-Harbor Agreement.</b></p>			
<p>14. Have internal controls been established at the company to help ensure compliance with applicable regulations? Please provide evidence of the</p>			

controls and a list of the personnel responsible for ensuring compliance.  
*Test procedure: the examiner's evaluation of the controls documentation will generally be sufficient for this test.*

**Guidance Point: The company's legal or compliance function should review the company's insurance coverage to ensure it covers e-commerce transactions. For example, the company needs to determine whether its insurance covers lost business due to Web site failures, the penalties from unauthorized disclosure of customer or business partner information, fines from violating privacy regulations and the costs associated with prosecuting security break-ins.**

15. Are the risks involved with the company's E-Commerce activities covered by an insurance policy? Please provide evidence of the insurance coverage.  
*Test procedure: The examiner's evaluation of the coverage will generally be sufficient for this test.*

**Guidance Point: Alliance management controls include the assignment of resources to manage the alliance, definition of the company's and the alliance partner(s) roles and responsibilities, maintenance of service level agreements (SLAs) and management of problem identification, investigation and resolution.**

16. Is there a control that service level agreements (SLAs) with e-commerce partners are actively monitored to ensure that IS responsibilities are appropriately managed? If so, please provide a copy of the SLAs and a copy of management policies and procedures. *Test procedure: The examiner's evaluation of the controls documentation will generally be sufficient for this test.*

Yes	No	Attachment

**Guidance Point: Operational Resilience – Effective operational resilience allows a company to significantly reduce business risk and avoid operational failure, including failure in operational process or strategy and operational lapses in control that endanger the company’s ability to achieve its strategic objectives. Operational failures can include the unavailability of operations or services and the inability to meet customer demands.**

**Scalability of Architecture – The ability to increase or decrease the network architecture, including software and hardware components, to meet changes in demand. The scalability of the company’s business model needs to be considered in conjunction with scalability of its e-commerce technical architecture. A scalable network architecture means the architecture can be changed in size and configuration without major changes needing to be made.**

**Redundancy – Means that if a primary component failure occurs, there is a redundant component that can take over in the event the primary component fails.**

**Load Balancing – The concept of distributing of processing across a network so that that no one device bears too much of the workload. Load balancing becomes more important in situations where web site traffic is difficult to predict. If the load is not balanced, network failures or delayed response time can occur. There are several methods of load balancing, e.g., hardware based, software based.**

**Performance Monitoring – The process in which key resources of a system are identified and then monitored on a continuous basis. Typically, the company should monitor network capacity, server capacity (CPU, memory, I/O capacity) and storage capacity. The company should have the ability to take snapshots of current performance in the environment (i.e., snapshot of a system’s CPU utilization at x time) and the ability to trend key measurements over a period of time (i.e., intra-day CPU utilization, weekly CPU utilization, monthly CPU utilization, etc).**

**Capacity Planning — Directly related to performance monitoring. With capacity planning, baseline values are derived from performance monitoring activities. These baselines are indicators of performance under normal loads as well as upper-level thresholds. The actual planning exercises use this information, gathered from performance monitoring, and input from business units on expected changes to the current volumes (e.g., from a marketing campaign or general market change) to create capacity planning models. These models are then used to determine if the current environment needs to be enhanced to support the future business needs**

Yes	No	Attachment

17. Have the following operational resilience elements been addressed for e-business initiatives?
- a. Scalability of architecture?
  - b. Redundancy?
  - c. Load balancing?
  - d. Performance monitoring?
  - e. Disaster recovery/business continuity?

Please provide evidence, showing that these elements have been addressed. *Test procedure: The examiner's evaluation of the documentation will generally be sufficient for this test.*

**Guidance Point: Authentication is the verification of a user's identity. Confidentiality is the assurance that stored and transmitted data can only be viewed by those people who are specifically authorized. Integrity is the assurance that stored and transmitted data is accurate and can only be modified by those people who are specifically authorized. Auditability is the ability of systems and applications to create and maintain useable records for all user actions and system events.**

**By definition, non-repudiation is the strength and accuracy of authentication, integrity, confidentiality and audit controls so users can or cannot deny the validity of their transaction. This is becoming a hot topic as the use of the Internet for electronic commerce increases. An example of non-repudiation occurs when you go to a grocery store and sign your check in front of the cashier. The cashier looks at the picture and signature on your driver's license and then compares them to your face and signature on the check. As a result, you cannot deny that you signed the check. (This example assumes that you can rely on the integrity of the driver's license and the integrity of the review performed by the clerk.)**

18. Has the company reviewed its business processes and controls and assessed its e-commerce security risks in terms of authentication, confidentiality, integrity, auditability and non-repudiation? Please provide a copy of this review and/or assessment. *Test procedure: The examiner's evaluation of the assessment documentation will generally be sufficient for this test.*

19. Has the company considered, documented and implemented a process for the creation, maintainability, and archiving of all the company's web content? Please provide a copy of the process. *Test procedure: The examiner's evaluation of the process documentation will generally be sufficient for this test.*

**Guidance Point: The company should address intellectual property rights in its contracts with third-party consultants. In addition, employee contracts should address intellectual property rights.**

Yes	No	Attachment

	Yes	No	Attachment
I10. a. Has the company established a strategy and supporting procedures to ensure that its intellectual property is adequately protected?			
b. Has management taken precautions through legal and technical means to protect the company's Web content?			
c. Does management ensure contracts with IT vendors and partners address intellectual property rights?			
Please provide a copy of the procedures document that describes management's approach to these issues. <i>Test procedure: The examiner's evaluation of the documentation will generally be sufficient for this test.</i>			
I11. Does company management take reasonable security precautions to ensure that personal data about the company's web site visitors is not accessible by unauthorized persons? Please provide a copy of the policy and procedures document describing management's approach to this issue. <i>Test procedure: The examiner's evaluation of the policy and procedures documentation will generally be sufficient for this test.</i>			
I12. Are there controls in place to ensure that the company's approved internet privacy policy is provided to all web visitors as required?  Please provide a copy of the company's corporate or divisional privacy policies. <i>Test procedure: The examiner's evaluation of the documentation will generally be sufficient for this test.</i>			
I13. Has company management created channels for the company's customers to provide electronic feedback about the company's products and services? Please provide a copy of the most recent summarization of electronic customer feedback. <i>Test procedure: The examiner's evaluation of the feedback documentation will generally be sufficient for this test.</i>			

Yes	No	Attachment

Guidance Point: (Source: PricewaterhouseCoopers E-Business Technology Forecast)

**PGP – Stands for Pretty Good Privacy and is a type of public-key encryption. A public key is essentially a binary number algorithm that locks and unlocks data. Public-key encryption is based on two keys: one to encrypt the message and another to decrypt it. Public key cryptosystems are also referred to as asymmetric key encryption, which means that knowing the public encryption key is no help in being able to decrypt a message. Users wanting to receive confidential information can freely announce their public key, which then is used by the sender to encrypt data to be sent to them. (Typically, public keys are stored in a publicly accessible standardized directory.) The data can be decrypted only by the holder of the corresponding private key.**

**Public Key Infrastructure (PKI) – “A PKI is the underlying technical and institutional framework that allows public-key encryption technology to be deployed widely...Integral to a PKI are a means of authentication and encryption, secure directory services, secure interoperation of directory servers and client access to directories, and the Simple Distributed Security Infrastructure (SDSI), a system that uses public-key cryptography combined with mechanisms for defining groups and group membership certificates. A PKI is designed to solve the problem of trustworthiness.”**

**Symmetric Key Encryption – “In the shared single-key method, the same key is used to encrypt and decrypt the message. However, this method requires that the sender and recipient both have the same key and that no one else does. Transmitting the key over the same insecure channel as the encrypted message is not acceptable, so a secure out-of-band communications method is required. (Even more critical to such an exchange is a preexisting relationship between the two parties that creates a secure context within which the secret-key can be exchanged.) Moreover, each pair of parties requires a unique key. The number of keys increases rapidly as the number of transactions grows. The most commonly used symmetric-key algorithms are the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), or Triple-DES.”**

**SSL – “The most popular process in use today to protect sensitive information such as payment data uses the Secure Sockets Layer (SSL) protocol, which was developed by Netscape and is now a de facto standard. SSL encrypts data sent between Customer Alice’s browser and Merchant Bob’s server. SSL constructs a communication connection where all data is encrypted before being transmitted over the Internet. Handshake routines at the onset of an SSL session share identifying information between the two parties, select one of several encryption algorithms to be used, and create the necessary session-specific encryption keys.**

**Alice’s browser, for example, must locate Bob’s public key, which is stored at Bob’s Web commerce site. Using Bob’s public key, Alice’s browser can create an encrypted message only Bob can read containing a unique, session-specific key that will be used to encrypt messages exchanged between the two parties**

for the duration of this transaction. After the handshake is completed, Alice's browser and Bob's server exchange data that is encrypted using conventional secret-key encryption before being transported over the insecure network. The entire process is transparent to Alice and Bob because the complex SSL technology has been embedded successfully in browsers and servers without burdening users with the need to understand or be involved in the setup of the secure data transfer."

I14. Does the company utilize encryption technology for securing its E-Commerce transactions? If yes, what forms of encryption and how are they used? Please provide documentation of the types of transactions and the types of encryption used, such as simple PGP, Secure Socket Layer (SSL), point-to-point hardware encryption or digital certificates in a Public Key Infrastructure (PKI). Please provide the contact information for a person responsible for encryption of e-business transactions. *Test procedure: the examiner's evaluation of the documentation, review of selected transactions and corroborating interviews will generally be sufficient for this test.*

**Guidance Point:** (Source: PricewaterhouseCoopers E-Business Technology Forecast.) If the company uses digital certificates in any form, then question I15 needs to be answered regarding the issuance, maintenance and deletion of certificates.

A certification authority is also referred to as a CA. "Certification authorities address the PKI problem by supplying authentication as a service from a trusted third party. The certification authority vouches for the authenticity of a public key either by storing it in a centralized, online database or by distributing it with a certificate, which is basically a copy of the user's public key that has been digitally signed by the certification authority. An enterprise may operate its own certification authority.

A certificate is similar to an identity card with a notary seal on it. It is valid for a stated period of time and is subject to cancellation by being included on a certificate revocation list (CRL). CRLs basically are "hot lists" that identify certificates that have been withdrawn, canceled, or compromised or that should not be trusted for other specified reasons."

I15. a. Does the company operate its own digital certificate authority (CA)?

b. Has the company outsourced that function?

Please provide documentation regarding all certificate management processes including a copy of the certificate practice statement and certificate policies. Please provide the contact information for a person responsible for management of digital certificates. *Test procedure: The examiner's evaluation of the documentation, review of selected transactions, and corroborating interviews will generally be sufficient for this test.*

Yes	No	Attachment

**J. NETWORK AND INTERNET CONTROLS**

The name, title and phone number of the insurance company's contact person responsible for providing the answers to this set of questions is:

---

	Yes	No	Attachment
J1. Does the company have documentation to identify and describe network nodes and network configurations? Please provide copies of historical and current network design and network configuration, and/or narratives describing network design and configuration. <i>Test procedure: The examiner's evaluation of the documentation provided will generally be sufficient for this test.</i>			
J2. Is the process used in changing the network configuration documented? Please provide a copy of the documented process and the name and phone number of all network administrators. <i>Test procedure: The examiner's evaluation of the process, corroborating inquiry with the person identified and observation of the process, if possible, will generally be sufficient for this test.</i>			
J3. a. Are controls in place to help ensure employee Internet usage is commensurate with the Internet usage policy?			
b. Is access to the Internet restricted so that inappropriate locations may not be accessed?			
<i>Test procedure: the examiner's evaluation of the evidence provided will generally be sufficient for this test.</i>			
J4. Is financially significant accounting information or sensitive management information transmitted across the network or Internet and, if yes, is a data encryption feature in place and functioning? Please provide the name of the data encryption package, the name of the person who has access to the keys and the name and phone number of the person who can demonstrate the feature. <i>Test procedure: The examiner's corroborating inquiry with the person identified and observation of the feature in use will generally be sufficient for this test.</i>			
J5. Does the company use firewall technology to protect its internal network from the external networks? Please provide the name and phone number of the person who can provide evidence of the use of firewall technology, including diagrams that show the firewall's location within the network infrastructure, as well as the protection rules for the firewall. <i>Test procedure: The examiner's corroborating inquiry with the person identified and observation of the technology in use will generally be sufficient for this test.</i>			
J6. Does the company scan all incoming e-mail, files and other network traffic for malicious content?			
Does the company disinfect e-mail, files and other network traffic from identified malicious content?			

Please provide a description of the detection technology and the name and contact information for the person who can demonstrate its use. *Test procedure: The examiner's corroborating inquiry with the person identified and observation of the technology in use will generally be sufficient for this test.*

- J7. Does the company scan or filter outbound e-mail for either offensive or potentially damaging content? Please provide the name of the content filtering technology and the name and contact information for the person who can demonstrate its use. *Test procedure: The examiner's corroborating inquiry with the person identified and observation of the technology in use will generally be sufficient for this test.*

Yes	No	Attachment

## ATTACHMENT A – SIGNIFICANT COMPUTER APPLICATIONS

Complete this schedule for all financially significant computer hardware and software.

Application Name	Application Function <sup>1</sup>	Computing Platform <sup>2</sup>	Application Software Source <sup>3</sup>	Date of Application Installation	Are changes Made to this Application?	Team Supporting Application <sup>4</sup>	Location(s) of Business Users	Location(s) of Computer Systems

<sup>1</sup> At a minimum, include systems responsible for general ledger functions, policy issuance, policy administration and claims/payment processing.

<sup>2</sup> Each unique computing platform should have a separate row entry in the table below.

<sup>3</sup> Application software source could be in-house development, external custom development, package or customized package.

<sup>4</sup> Please indicate if this application is outsourced, supported in a remote data center or completed by a separate IS organization.

Operating System	Platform	OS Security Software <sup>5</sup>	Hardware Location

<sup>5</sup> e.g., RACF, ACF2, Top Secret, OS400, Windows 2000, Novell, Linux, Unix, etc.

## ATTACHMENT B – SERVICE PROVIDER QUESTIONNAIRE (COMPLETE FOR EACH SERVICE PROVIDER)

<b>Service Provider Name</b>	<b>Number of years in business</b>	<b>Managing executive of the service provider</b>	<b>Name, title and phone number of the insurance company contact at the service provider</b>	<b>Name, title and phone number of the individual within the insurance company designated to be the liaison with service provider</b>

**Attach copies of all executed current contracts between the service provider and the company and answer the following questions:**

	Question	Yes	No	Attachment
1	Does the service provider have an independent, external auditor and, if so, provide a copy of the most recent SAS-70 and/or Sarbanes-Oxley report, management letters, and the service provider's response.			
2	Does the contract allow the insurance company to conduct audits?			
3	Has the service provider been audited by the insurance company and, if so, provide a copy of the most recent IS internal audit report and the service provider's response			
4	Does the service provider provide any of the following services for the insurance company?			
	a. Processing?			
	b. Data preparation?			
	c. Program development?			
	d. Program maintenance?			
	e. Systems analysis?			
	f. Other (explain)?			
5	Does the service provider's blanket bond (fidelity insurance) cover losses due to actions by their personnel? Please provide a copy of the service provider's blanket bond or evidence that auditing and testing of the bond is included in the SAS-70 report completed by the service provider's external auditors. <i>Test procedure: The examiner's evaluation of the bond or evidence from the SAS-70 report will generally be sufficient for this test.</i>			
6	Does the service provider carry insurance adequate to restore loss of company records due to mishap? Please provide a copy of the service provider's insurance policy covering the loss of company records due to mishap or evidence that auditing and testing of the policy is included in the SAS-70 report completed by the service provider's external auditors.			

## ATTACHMENT B – SERVICE PROVIDER QUESTIONNAIRE (COMPLETE FOR EACH SERVICE PROVIDER)

	<b>Question</b>	<b>Yes</b>	<b>No</b>	<b>Attachment</b>
<b>7</b>	Is the service provider adequately protected by a disaster plan and, if so, is it up-to-date and tested? Please provide a copy of the service provider's disaster recovery plan and related test results or evidence that auditing and testing of the disaster plan and related test results is included in the SAS-70 report completed by the service provider's external auditors. <i>Test procedure: The examiner's evaluation of the disaster recovery plan and related test results or evidence from the SAS-70 report will generally be sufficient for this test.</i>			
<b>8</b>	Have provisions been made for backup of critical files away from the service provider premises? Please provide a copy of the service provider's backup procedures or evidence that auditing and testing of the backup procedures is included in the SAS-70 report completed by the service provider's external auditors. <i>Test procedure: The examiner's evaluation of the backup procedures or evidence from the SAS-70 report will generally be sufficient for this test.</i>			
<b>9</b>	Does the company maintain the original or a copy of all source documents transmitted to the service provider? Please provide a copy of the source documents for the last transmission to the service provider that occurred during the period under review. <i>Test procedure: The examiner's evaluation of the source documents provided, as well as source documents for a judgmental sample of transactions processed within the past 12 to 24 months, will generally be sufficient for this test.</i>			
<b>10</b>	Are controls, such as document count, transaction count or other control totals, established for all documents sent to or handled by the service provider? Please provide a description of the controls and the name and phone number of the person who can validate the controls. <i>Test procedure: The examiner's evaluation of the controls, corroborating inquiry with the person identified and observation of the controls, if possible, will generally be sufficient for this test.</i>			
<b>11</b>	Are input control figures reconciled with the control figures furnished by the service provider? Please provide a copy of a recent reconciliation that occurred during the period under review. <i>Test procedure: The examiner's evaluation of the reconciliation provided, as well as a judgmental sample of reconciliations performed within the past 12 to 24 months, will generally be sufficient for this test.</i>			
<b>12</b>	Are all rejected transactions clearly identified and listed on an error report or file? Please provide a copy of the last printout made during the period under review. <i>Test procedure: The examiner's evaluation of the printout provided will generally be sufficient for this test.</i>			
<b>13</b>	Are there methods to ensure that errors are corrected by the service provider? Please provide a copy of the error resolution procedures and the name and phone number of the person who can demonstrate or validate the methods. <i>Test procedure: The examiner's evaluation of the controls corroborating inquiry with the person identified and observation of the controls, if possible, will generally be sufficient for this test.</i>			