

March 18, 2008

TO: NAIC Advisory Organization Examination Protocol Working Group:

At the January 31 teleconference call of the working group you requested comments from interested parties relating to the drafts of the statistical agent/advisory organization examination including the draft Information Systems Questionnaire (ISQ) and the proposed Chapter 16 – General Examination Standards. ISS appreciates the opportunity to offer our comments. While we still have concerns about many of the latter items in Chapter 16, as they do not seem to fit with statistical/advisory organization activities, we would like to limit our comments to the ISQ, and to Chapter 16 items 2 and 4, which appear to address various aspects of the ISQ.

As ISS communicated last year to the ISQ subgroup, it is our opinion that some of the items included in the current ISQ draft titled "Information System Controls RSM edits.pdf" appear to go beyond the scope of a statistical agent and/or advisory organization examination. This scope is defined under "Section 2. Nature, Scope and Type of Examination" as detailed in the current draft of Chapter 25 – Conducting the Statistical Agent Examination. The scope is best summarized by the following excerpt: *"The main purpose of the examination is to look at what the advisory organization does with the data it collects, compiles and reports so that state regulators know that the statistical, loss costs, rule and form filings made with them are accurate and reliable."* We believe there are four corporate functions related to the integrity and security of the processing environment that address the intended scope and therefore could be included in an examination. These are: management and organizational controls, logical and physical security, the management of systems applications, and disaster recovery, contingency planning.

We offer three attachments to this letter that we believe address our concerns. The first attachment is a new proposed version of an Information Systems Questionnaire. We believe that it addresses the intended scope of the examination as it relates to IS applications and systems of statistical/advisory organizations. Examination of the four functions is addressed by the four sections of our proposed ISQ. We extracted the relevant items from the previous ISQ and reworded them to apply specifically to statistical/advisory organization functions. We then removed items that seem to go beyond the scope as we understand it from Section 2 as noted above. We believe this ISQ offers an appropriate level of assurance that statistical/advisory organizations have the proper controls in place over the IS environment as it relates to the statistical agent and ratemaking systems.

The second attachment is a spreadsheet framework for responding to the ISQ. We thought it might be easier to work with this as a document separate from the ISQ itself.

The third document includes reworded standards 2 and 4 from Chapter 16, with revised review procedures and criteria that relate to our proposed ISQ.

We appreciate the opportunity to provide these comments and proposed changes, and hope that the working group will take them under consideration. We will be happy to answer any questions from the working group.

Respectfully,



Stuart A. Yakes
Vice President, ISS

Attachment 1

A. MANAGEMENT AND ORGANIZATIONAL CONTROLS

NOTE: Management and Organization Control questions must be completed for each of the statistical/advisory organization's significant organizational units that are directly responsible for maintenance or development, operation or security of significant statistical and ratemaking 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 statistical/advisory organization's contact person responsible for providing the answers to this set of questions must be included on the response summary.

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.

Test Procedures: The examiner's evaluation of the documentation provided will generally be sufficient for this test.

- A1. 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.
- A2. Are the IS roles and responsibilities clearly defined and separate from the operations and/or user departments? Provide job descriptions which explain the separation of functions between
 - IS and other operating departments within IS
 - Application development/maintenance and Operations
- A3. Are routine audits performed either by internal audit staff or outside consultants? If so, on what frequency? Provide contact information and audit reports for the most recent audit of a significant production system.

B. LOGICAL AND PHYSICAL SECURITY

NOTE 1: Logical and Physical Security questions will 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 statistical/advisory organizations 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 significant statistical and ratemaking systems. However, some statistical/advisory organizations may rely upon application-based security to restrict access to appropriate functions within significant production applications while other organizations may rely upon system-based security to secure both system access and application access. If the organization under examination relies upon system-based security to secure both system access and application access, questions B12 – B15 should be skipped.

The name, title and phone number of the statistical/advisory organization's contact person responsible for providing the answers to this set of questions and conducting a facility tour must be included on the response summary.

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.

Test Procedures: The examiner's evaluation of the documentation provided and observation of the facility will generally be sufficient for this test.

PHYSICAL SECURITY

- B1. a. What physical access controls are in place to secure the computer/communication facilities
- Data Centers
 - Server Rooms
 - Wiring Closets
 - Tape Libraries
- b. 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?
- c. Are computer/communication facilities protected from damage resulting from electronic power interruption, surges and spikes?
- B2. Are access procedures in place to ensure that only authorized individuals are being permitted to enter the facility? Include necessary documentation/logs to demonstrate access control.
- B3. Is there a process for maintaining a current list of authorized individuals with access to sensitive computer/communication facilities? Provide documentation of the request and the procedure followed for additions, changes and deletions.

Guidance Point: Only appropriately authorized individuals should be granted access to system resources. Access should be granted by the security administrator after the appropriate approvals have been obtained from management. Update access to the claims master data file, outside of the application software (e.g., by writing independent programs), should only be granted if approval has been obtained from appropriate management. When employees are transferred between departments, their access privileges to system and application resources should be updated accordingly. When employees are terminated, all system access privileges should be revoked immediately. Finally, the company’s management should expressly prohibit the sharing of user IDs and passwords.

Test Procedures: The examiner’s evaluation of the documentation provided and corroboration with security personnel will generally be sufficient for this test.

LOGICAL SECURITY – System/Environment Access

- B4. a. Is there a system level control that ensures effective system password management (e.g., unique user IDs, passwords)?
 - b. Are passwords generated by each user rather than assigned by the company?
 - c. Are passwords properly masked during the logon process and omitted from printed output?
 - d. Are passwords stored in an encrypted state and not viewable by security administrators?
 - e. Are passwords transmitted in an encrypted state across the network during the authentication and authorization process?
 - 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 copy of the logical security procedures used to manage password and to determine the structure and use of system passwords (e.g., password expiration, password composition and password confidentiality) and the name and number of the person who can demonstrate system security settings.

- B5. 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 copy of the procedures and evidence that the procedures were followed for the most recent IS person or user initialized during the period under review.

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.

- D6. Does user department management periodically validate the access capabilities provided to individuals in their department? Please provide evidence of the last user access review performed during the period under review.
- B7. 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.

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.

- B8. 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.
- B9. 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.
- B10. 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.

LOGICAL SECURITY – Application Access

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.

Test Procedures: The examiner’s evaluation of the documentation provided and corroboration with security personnel will generally be sufficient for this test.

- B11. 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.
- B12. Is there an application level control that ensures effective application password management (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.
- B13. 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 significant statistical and ratemaking application.
- B14. Are periodic checks carried out to confirm that employees’ current application access is commensurate with their job responsibilities? Please provide evidence of the last check performed during the period under review.
- B15. Are there procedures that ensure that application 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.

Guidance Point: 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. Emergencies during the day can be corrected by a responsible technical support person with a user-ID with special privileges. Problems outside normal working hours, the off-shift personnel (e.g., on-call programmer) may need a special user ID.

16. 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.

SECURITY – Monitoring & Management

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.

Test Procedures: The examiner’s evaluation of the documentation provided and corroboration with security personnel will generally be sufficient for this test.

- B17. 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.
- B18. 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.
- B19. If wireless technologies are deployed, does the company monitor for rogue access points? Please provide the most recent scan for rogue access points.
- B20. 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)? 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.
- B21. Is sensitive 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.
- B22. 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.

- B23. 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.

C. APPLICATION MANAGEMENT

NOTE: Section C must be completed if the company develops new and/or changes existing statistical agent and ratemaking applications. These questions apply to in-house developed systems as well as purchased applications.

The name, title and phone number of the statistical/advisory organization's contact person responsible for providing the answers to this set of questions must be included on the response summary.

Test Procedures: **The examiner's evaluation of the documentation provided will generally be sufficient for these tests.**

- C1. Is there a control that ensures that user needs result in appropriate program change requests and the requests are properly developed? Please provide a list of all program change requests made during the period under review.
- C2. Do user departments, auditors, operations, and system architect personnel participate in the early stages of requirements definition and planning for new system and/or major enhancements to ensure accurate scope and detailed business needs? Provide evidence of involvement of all parties in the projects.

Guidance Point: **A well-controlled advisory organization and/or statistical agent 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 testing would tend to cover the areas noted above, as well as between specific subsystems.**

- C3. Is appropriate program, system and parallel (when possible) testing performed by the IS staff and QA/User staff to prevent or detect errors in program coding and ensure that the application operates as intended in the production environment and provides accurate data output? Provide test results from recent projects.

Guidance Point: **A well-controlled advisory organization and/or statistical agent has procedures in place to ensure that program code is migrated from one environment to another with a controlled process that does not allow the developers to migrate their own programs to the production environment. Additionally, management should be aware of all production migrations.**

- C4. a. Is there a control that ensures that the correct program libraries (at all processing sites, if appropriate) are updated with the most recent version of the program after user testing is complete? Please provide a description of the control and the name and phone number of the person who can demonstrate or validate the control.
- 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.
- C5. Is program code secured for access by only authorized individuals? Describe staging procedures to secure directories, datasets or other containers of source code during the transition from development to production (stages include: in development, in testing, tested – waiting for production migration, in production).

- C6. 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.
- 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.
- C7. Is user documentation appropriately updated and distributed to affected users? Please provide a copy of updated documentation for the most significant program change made from question C1.

D. DISASTER RECOVERY / CONTINGENCY PLANNING

The name, title and phone number of the statistical/advisory organization's contact person responsible for providing the answers to this set of questions must be included on the response summary.

Test Procedures: The examiner's evaluation of the documentation provided and corroboration with disaster recovery personnel will generally be sufficient for this test.

D1. Are the statistical agent and ratemaking files and databases routinely backed up? Please provide a copy of the backup schedule for files and databases related to the significant applications.

D2. Are copies of the application, data file/database backups, essential statistical agent and ratemaking documents and/or business records stored offsite? 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. Also provide a copy of the Data Center backup management process which includes the frequency of offsite delivery.

D3. Is the disaster recovery/business contingency plan:

- current;
- based on a business impact analysis;
- tested periodically; and
- developed to address statistical agent and ratemaking functions and related 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.

D4. 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.

D5. a. Does the plan contain a list of critical statistical agent and ratemaking 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 a copy of the plan.

D6. Has a restoration priority been assigned to all significant statistical agent and ratemaking activities? Please provide a copy of the prioritized activities.

D7. 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 user area who can demonstrate the procedures.

D8. 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.

D9. a. 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?

b. 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

Attachment 2

Information System (IS) Questionnaire

Section	Question	Response		Attachments	Comments
		Yes	No		
A. Management and Organizational Controls					
Contact Name/Phone:					
	1				
	2				
	3				
B. Logical and Physical Security					
Contact Name/Phone:					
Physical	1.a				
	1.b				
	1.c				
	2				
	3				
Logical - System Access	4.a				
	4.b				
	4.c				
	4.d				
	4.e				
	4.f				
	5				
	6				
	7				
	8				
Logical - Application Access	9				
	10				
	11				
	12				
	13				
	14				
Monitoring & Management	15				
	16				
	17				
	18				
	19				
	20				
	21				
	22				
	23				

Information System (IS) Questionnaire

Section	Question	Response		Attachments	Comments
		Yes	No		
C. Application Management					
Contact Name/Phone:					
	1				
	2				
	3				
	4.a				
	4.b				
	5				
	6				
	7				
D. Disaster Recovery / Contingency Planning					
Contact Name/Phone:					
	1				
	2				
	3				
	4.a				
	4.b				
	4.c				
	5.a				
	5.b				
	6				
	7				
	8				
	9.a				
9.b					

Attachment 3

**STANDARDS
OPERATIONS/MANAGEMENT**

Standard 2

The regulated entity has appropriate controls, safeguards and procedures for protecting the integrity of computer systems and information.

Apply to: All regulated entities

Priority: Essential

Documents to be Reviewed

_____ Applicable statutes, rules and regulations

_____ Electronic records control, ~~recovery/backup plan~~ and regulated entities' procedural manuals;
~~whether the records are electronic~~

_____ Negotiated contracts

Others Reviewed

NAIC Model References

Privacy Protection Model Act

Health Information Privacy Model Act

Review Procedures and Criteria

~~Review regulated entity records, central recovery and backup procedures. The plan and procedures should be valid and up to date. (moved concept to # 4)~~

Review physical security procedures (ISQ Section B) related to the computer processing facilities and the network:

- Confirm that the computer/communication facilities (computer room, network operations center, wiring closets, etc) are secure and protected from hazards.
- Confirm that access to the computer/communication facilities is restricted to only authorized personnel at all times.
- Confirm that the regulated entity uses firewall technology to protect its internal network from unauthorized external access
- Confirm that the regulated entity scans inbound messages and files for malicious content
- Confirm that the regulated entity encrypts sensitive data files when transmitting data outside the physical premises

Review logical security and computer system control procedures (ISQ Section B)

- Confirm that access to the regulated entity's network and computer systems is protected minimally with unique user IDs and passwords, based upon the sensitivity of the information and the requirements of the individuals.
- Confirm that computer programs/databases/files impacted by user change requests are properly monitored, modified, tested and migrated to the secure production libraries.

~~If the regulated entity permits changes to be made to policies either electronically or verbally, check what security procedures the regulated entity has established to permit these changes. These may include who has authority to make those changes, and what verification is done by the regulated entity with the insured after changes are made.~~

~~Ensure there is adequate security of applicant/insured data during the electronic transference of information. Identify any areas where the applicant's/insured's privacy is not properly protected.~~

Review the segregation of duties between the Application Development, Operations and User departments to confirm that IS projects are authorized, controlled and documented. (ISQ Section A)

Confirm that changes to the Application portfolio are authorized, controlled and documented. (ISQ Section C):

- Confirm that user departments review, approve and sign-off on the implemented changes and the test results prior to the migration to the production environment.
- Confirm that there are sufficient controls in the migration of new application components to the production environment which guarantee accuracy and completeness

STANDARDS

**OPERATIONS/MANAGEMENT
STANDARDS
OPERATIONS/MANAGEMENT**

Standard 4

The regulated entity has a valid disaster recovery plan.

Apply to: All regulated entities

Priority: Essential

Documents to be Reviewed

_____ Applicable statutes, rules and regulations

_____ Description of the regulated entity's disaster recovery plan, procedural manuals and controls

_____ ~~Description of protective devices for various hazards and procedures/controls for protection from those hazards~~

_____ Negotiated contracts

Others Reviewed

NAIC Model References**Review Procedures and Criteria**

~~Determine that the regulated entity's database(s) are protected from various hazards, including environmental hazards. (moved concept to #2)~~

Ensure that critical business applications, databases and files are regularly backed up and stored off-site.(ISQ Section D)

Review the disaster recovery plan and procedures:

- Confirm the recovery procedures are current, detailed and repeatable
- Confirm the inventory of critical business applications, database and files is current and is defined and prioritized in the recovery process
- Confirm that critical business areas developed manual processing procedures to be deployed while the computing environment is unavailable
- Confirm that the regulated entity completes disaster recovery testing (offsite retrieval through restoration of a fully operational computing environment) on a regular basis

~~Review the regulated entity's documents. Any additional areas or lack of information should be discussed with the regulated entity's management. The disaster recovery plan should be valid, specific and operational, with procedures for implementation and should also be current. Failure of the regulated entity to adequately plan for the future means the standard was not met.~~

~~Failure of the regulated entity to adequately (on an ongoing basis) provide for off-site backup, failure of the regulated entity to provide adequate controls and, in the case of a catastrophe, failure to provide for recovery, means the standard was not met.~~

~~Standard #2 of this section also addresses disaster recovery issues.~~