Government of the District of Columbia
Department of Insurance, Securities and Banking

Stephen C. Taylor
Commissioner

BEFORE THE
INSURANCE COMMISSIONER OF
THE DISTRICT OF COLUMBIA

Re: Report on Examination – **American Association of Insurance Services**

ORDER

In accordance with the authority established by D.C. Official Code § 31-2708(a)(1), a Market Conduct Examination of **American Association of Insurance Services** as of December 31, 2015 has been conducted by the District of Columbia Department of Insurance, Securities and Banking ("Department") as a participating jurisdiction through the National Association of Insurance Commissioners' Advisory Organization Examination Oversight (C) Working Group. The Department accepts the report in lieu of a single jurisdiction examination.

It is hereby ordered on this 14th day of December 2017, that the attached Market Conduct Examination Report be adopted and filed as an official record of this Department.

Pursuant to D.C. Official Code § 31-1404(d)(1), this Order is considered a final administrative decision and may be appealed.

Pursuant to D.C. Official Code § 31-1404(e)(1), the Department will continue to hold the content of the report as private and confidential information for a period of 10 days from the date of this Order.

Stephen C. Taylor
Commissioner

Illinois Department of Insurance

BRUCE RAUNER
Governor

JENNIFER HAMMER
Director

VIA FIRST CLASS MAIL AND ELECTRONIC MAIL

November 20, 2017

Edmund J. Kelly, President
American Association of Insurance Services
701 Warrenville Road
Lisle, IL 60532

Re: American Association of Insurance Services (AAIS or Association)
Market Conduct Examination Final Report

Dear Mr. Kelly:

On July 17, 2017, the Department sent AAIS a draft copy of the examination report for the above examination. On November 8, 2017, the Department received correspondence from Robin Westcott, Esq., Vice President and General Counsel of AAIS, accepting the findings contained in the report as revised and presented to AAIS on November 7, 2017.

Enclosed with this letter is a copy of the final verified examination report. No order will be issued by the Department in conjunction with this report. The Department will transmit the report to the Advisory Organization Examination Oversight Working Group of the National Association of Insurance Commissioners for consideration and adoption by the other states participating in the multistate examination.

At this time the examination is considered concluded by the Department and the report of examination is considered filed. The Department would request, however, being updated as to the status of AAIS filling its chief auditor position once the search is completed.

The examination report is now considered a public document under the Freedom of Information Act ("FOIA") [5 ILCS 140/1 et seq.] and may be posted to the Department's website. To the extent that the examination report contains information that AAIS deems private, personal or trade secret pursuant to Sections 7(1)(b), (c), or (g) of FOIA [5 ILCS 140/7(b), (c), and (g)], AAIS may request that the Department redact such information from the report prior to making it public. In making a request for confidentiality, AAIS must provide a basis for its assertion of confidentiality. The Department will consider the request and determine whether such information is exempt from disclosure under Section 7 of FOIA.

Thank you for AAIS' cooperation throughout this process. Please contact me if you have any questions.

Sincerely,

Michael P. Rohan, JD, MCM
Deputy Director
Consumer Education and Protection
Illinois Department of Insurance
122 S. Michigan Avenue, 19th Floor
Chicago, IL 60603
Phone: 312-814-8206
E-mail: Michael.Rohan@Illinois.gov

cc: Robin Westcott, Esq.

REPORT OF EXAMINATION

As of December 31, 2015

AMERICAN ASSOCIATION OF INSURANCE SERVICES

701 Warrenville Road
Lisle, IL 60532

Report Issued November 20, 2017

TABLE OF CONTENTS

I. PURPOSE AND SCOPE OF EXAMINATION

The Advisory Organization Examination Oversight (C) Working Group of the National Association of Insurance Commissioners ("NAIC") initiated a targeted multistate examination (the "Examination") of the business practices of the American Association of Insurance Services ("AAIS" or the "Organization"). The period of the Examination is as of December 31, 2012, and includes any new matters raised by the NAIC Comprehensive Annual Analysis ("CAA") form completed by AAIS for calendar year 2015 (the "Period"). The primary purpose of the Examination was to determine compliance with applicable statutory and regulatory requirements and specifically, compliance with the findings of the most recent prior examination of AAIS. Illinois law and the relevant Standards of Chapters 16 and 25 and Appendix F of Chapter 25 of the NAIC's Market Regulation Handbook ("Handbook"), were referenced during the Examination.

The Examination was performed at the direction and overall management and control of the Illinois Department of Insurance (the "ILDOI" or the "Lead State"). Representatives from the firm of Risk & Regulatory Consulting, LLC ("RRC" or "the Examiners") were engaged to complete certain examination procedures.

RRC personnel participated in this Examination in their capacity as Examiners. The Examination Team included Actuarial, Information Technology ("IT") Specialists and Market Conduct Examiners. RRC provides no representations regarding questions of legal interpretation or opinion. Determination of Findings, if any, constituting potential areas of non-compliance are the sole responsibility of the Lead State. The Examination Report (the "Report") describes the review of practices, procedures and files, which was not exhaustive or all-inclusive; thus the omission of other unacceptable or non-complying practices does not constitute acceptance of these practices.

II. ORGANIZATION PROFILE

AAIS was organized in 1975 as an advisory organization and has grown, both in the products and services the Organization offers, and in the number of insurers it serves. AAIS is both an advisory organization and statistical agent licensed in all 50 states providing statistical agent services to more than 700 property & casualty insurers. The Organization makes statistical submissions to regulators in accordance with the NAIC Handbook of Information Available to Regulators ("NAIC Handbook"). AAIS also prepares and files advisory prospective loss costs, policy forms and manuals of rating rules for several lines of property & casualty insurance.

AAIS currently provides services related to the following: forms, manual rules, and rating information for more than 34 programs of personal, commercial, agricultural, and inland marine insurance; statistical reporting plans for programs the Organization supports, plus auto; and support services for actuarial analysis, automation, custom product development, state filings, and training. Services also include the AAIS Underwriting Platform, a cloud-based application introduced in 2013 for underwriting and rating policies based on AAIS programs, and for collecting the data generated in those transactions.

III. EXECUTIVE SUMMARY

A prior multistate examination of AAIS was called in October 2012, for the examination period of January 1, 2010 through September 30, 2012. The Lead States included Illinois (Managing Lead State) and Maine. RRC was retained to assist with conducting this examination. During this prior examination, the Examiners identified the Organization was in the process of transitioning to new leadership and significant changes in the Organization's actuarial and information technology (IT) areas were underway.

After assessing AAIS' status in 2012, RRC provided an update to the Lead States and the NAIC recommending that the examination should be suspended until AAIS had completed their reengineering process. The NAIC and the Lead States also concluded additional work should be suspended and RRC was directed to prepare a preliminary Examination Report noting findings and recommendations.

The current Examination, which was designated as a targeted multistate examination, was called by the NAIC on August 1, 2016. Illinois served as the Lead State and all 50 states agreed to be identified as Participating States. The primary purpose of the Examination was to focus on the Organization's status since the prior examination and how AAIS responded to the findings and recommendations from the prior examination.

IV. GENERAL OBSERVATIONS and CONCLUSIONS

The following is a high level summary of certain observations and conclusions identified during the Examination. Each of these observations are discussed in detail later in the report.

Actuarial

- The Examiners determined that AAIS' processes and procedures related to its regulated operations adequately meet the Handbook Standards reviewed during the Examination.
- AAIS has strengthened its actuarial operations since the prior examination, with the addition of credentialed actuaries and the implementation of a peer review process.
- The Organization's loss cost filings lack sufficient documentation to fully meet actuarial standards of practice (ASOPs). (Please reference Appendix II for specific commentary on AAIS's documentation as it relates to relevant ASOPs).
- AAIS's peer review process appears to be thorough and complete, but is not centralized and is not easily accessible from a documentation standpoint.
- AAIS is challenged to produce loss cost filings on a regular, annual basis for each line of business due to staffing limitations and the effort required to validate the data used for the loss cost analyses.

Information Technology

- To address needed improvements in the Organization's accuracy and reliability of its IT operations since the prior examination, AAIS has transitioned its IT infrastructure to include the following:
    - Replaced its antiquated AS/400 platform with current technology and implemented Agile (see background below) methodology for operations management.

- Improved its Disaster Recovery Plan ("DR Plan") by implementing a cloud-based environment located in a state of the art data center which is maintained by an independent third party.
- Improved its network infrastructure through the implementation of a Cisco Security Plus Firewall, which is monitored and generates alerts based on configured thresholds.
- AAIS improved its change management process through the implementation of Source Code management and Release Management utilities and the integration of those utilities into its processes.

- The IT department is not truly independent of the operating units for which it performs data processing functions. The Data Engineering group is organized under the Vice President - Chief Actuary who also manages the main users of the statistical data. It is noted that functions within the IT department (development vs. operations) are segregated.
- Currently, AAIS does not employ a consistent, independent function to provide quality control checks and balances (e.g., an Internal Auditor or internal audit-like function). Peer reviews are performed on a periodic basis based on risk areas that are self-identified by management; however, there are no processes currently in place to identify areas which could benefit from a more formal independent review.
- The process for performing the annual user access review needs to be revamped. Currently, user access is tracked in spreadsheets which are maintained by the Organization's Human Resource area and reviewed by relevant management personnel. Updates to the spreadsheets are made based upon access requests; however, these spreadsheets may not be an accurate reflection of the current production environment, the result of which means that managers may not be approving the actual level of access that has been granted to each user.
- IT activities are not consistently tracked in the same place using the same technology. For example, some significant tasks are tracked in Rally, while other tasks are tracked in ManageEngine. This lack of consistency may increase the risk of IT activities not being managed in a consistent manner or reported consistently for future tracking purposes.
- As of 2015, virus definitions for Apple Macintosh computers are dependent upon the user initiating any updates.
- The DR Plan does not contain sufficient detail to facilitate the timely restoration of processing for an application(s) on a consistent basis and testing of the DR plan is not performed on a consistent basis.
- There is no documentation to confirm that management reviews the Service Organization Controls ("SOC") report for Amazon Web Services ("AWS") or adequately monitors the activities of the contracted entity.

V. EXAMINATION METHODOLOGY

The Examiners primarily relied on the review of documentation and testing of records and information maintained by the Organization concerning certain of their operations included within the scope of the Examination. Also, the Examiners participated in AAIS presentations, which provided an overview of the Organization's operations. The Examination included Actuarial, IT and Market Conduct professionals.

During the Examination, Examiners' reviewed documentation and related information, for which included the Examiner's tendering individual Requests for Information ("RFIs), which the Organization provided complete and timely responses.

RRC's Actuarial Examiners work included reviewing AAIS' work product related to loss cost/rate filings (the "Filings"), with specific emphasis regarding the Organization's assumptions in preparing the Filings as well as the completeness and accuracy of the information. The Actuarial Examiners conducted interviews of the Organization's key actuarial resources, including the Chief Actuary.

The Market Conduct (MC) Examiners work focused primarily on a high level review of the Organization. Consistent with the prior examination and information documented in the CAA, no specific MC Standards were included with the scope of the Examination. The MC Examiners accomplished their work by the review of documentation, the Organization's practices and procedures, participating in interviews and leveraging the work of our Actuarial and IT Examiners.

RRC's IT Examiners approach and methodology was planned to gain a comprehensive understanding of the Organization's IT and Data infrastructure operations and as such, procedures included a focus on the design, implementation and operating effectiveness of the Organization's IT processes and associated IT general controls.

The IT Examiners also utilized appropriate questionnaires to accumulate the Organization responses and execute engagement start-up activities. The primary information-gathering document during this step was the RFI and also included a review of the prior examination report and internal management testing documentation and work papers. RRC also reviewed all IT-related information provided in response to the Initial Request for Information. Supporting documentation and information was provided by the Organization, including network diagrams, policies and other related documents.

The IT Examiners also conducted specific walkthroughs of certain AAIS systems and applications, including, but not limited to Rally and ManageEngine and reviewed information related to the AWS. Additionally, interviews and process walkthroughs with representatives of the Organization were also conducted. Targeted testing was performed consistent with the examination processes and sampling methodologies in concert with the Handbook guidance. Where appropriate, the Examiners tendered requests and follow-up inquiries, to the Organization for response.

VI. REVIEW OF EXAMINATION STANDARDS AND RESULTS

The Examiners reviewed and tested where applicable, the Standards included in the examination plan and Chapter 25 of the Handbook. Additionally, aspects of Appendix F of Chapter 25 of the Handbook were also referenced during the Examination.

Standard 2 - The advisory organization uses sound actuarial principles for the development of prospective loss costs.

Results: Standard Met

Observations: The Examiners performed a procedural review and testing to address the scope of Standard 2, which included a review of a sample of loss costs. Each sample was tested against certain actuarial guidelines set forth in the Actuarial Standards of Practice (ASOP), and identified below for reference:

- ASOP #12: Risk Classification (*Please see comment below*);
- ASOP #13: Trending Procedures in Property/Casualty Insurance;
- ASOP #23: Data Quality;
- ASOP #25: Credibility Procedures;
- ASOP #29: Expense Provisions in Property/Casualty Insurance Ratemaking (Loss Adjustment Expenses only);
- ASOP #38: Using Models Outside the Actuary's Area of Expertise (Property and Casualty);
- ASOP #39: Treatment of Catastrophe Losses in Property/Casualty Ratemaking; and
- ASOP #41: Actuarial Communications.

The Examiners' testing included a sample of calculations performed by AAIS, which were used to support the derivation of certain loss costs/rates including:

- Loss Development Factors;
- Premium Development Factors;
- Premium On-level Factors;
- Trend Factors;
- Credibility Procedures;
- Loss Adjustment Expenses;
- Classification Relativity Analysis; and
- Use of Models.

The Examiners relied on a judgmental sampling process, to select a sample of loss cost filings from a list provided by AAIS for the Period. The following table identifies the 12 loss cost filings tested for the year 2015.

Sample	State	Line of Business	Filing Designation
LC Filing 01	Utah	Homeowners	AAIS-2015-24LC
LC Filing 02	Missouri	Homeowners	AAIS-2015-24R
LC Filing 03	Delaware	Businessowners	AAIS-2015-16R
LC Filing 04	South Dakota	Businessowners	AAIS-2015-16R
LC Filing 05	Wisconsin	Businessowners	AAIS-2015-16R
LC Filing 06	Oklahoma	Businessowners	AAIS-2015-16R
LC Filing 07	Georgia	Businessowners	AAIS-2015-16R
LC Filing 08	Minnesota	Businessowners	AAIS-2015-16R
LC Filing 09	New Hampshire	Businessowners	AAIS-2015-16LC
LC Filing 10	Massachusetts	Terrorism Risk Insurance (TRIA)	AAIS-2015-3R
LC Filing 11	Illinois	Businessowners	AAIS-2015-16LC
LC Filing 12	Virginia	Homeowners	AAIS-2015-24LC

The Examiners selected three additional loss cost filings from the years 2013 and 2014, specifically to understand differences in AAIS's loss cost analysis procedures over the course of the Period. The additional loss cost filings are identified in the table below:

Sample	State	Line of Business	Filing Designation
LC Filing 13	Texas	Inland Marine	AAIS-2013-32LC
LC Filing 14	New York	Inland Marine	AAIS-2014-37LC
LC Filing 15	Maryland	Farmowners	AAIS-2014-77FOR

Please see Appendix I for summaries of the individual testing attributes and the rate filing testing information. Our most significant observation and recommendation from our testing of the loss cost filings is that AAIS should improve its documentation in the loss cost filings in order to be in full compliance with the relevant ASOPs, particularly ASOP 41, *Actuarial Communications*.

Please see Appendix II for a comparison of the overall indicated and selected loss cost change for each loss cost filing included in the testing. It can be observed in Appendix II that it is common for AAIS to temper the selected loss cost change when the indicated loss cost change is relatively large. This is not an uncommon business practice, but it may suggest that AAIS should consider changes in its credibility procedures, to help to ensure there is a higher degree of stability in the indicated loss cost changes.

Standard 12 - The advisory organization has an up-to-date, valid internal or external audit program.

Results: Standard Not Met

Observations: In its response to the NAIC's Comprehensive Annual Analysis (CAA) for 2015, AAIS stated the following: *"AAIS implemented an internal and external audit program in July 2013. No changes have been made to the program since that date. The AAIS Internal Audit Program is built upon the following components."*

- A review of company goals and strategic initiatives to guide the analysis of our policies and processes and recommended realignments or improvements.
- NAIC Chapter 25 Standards for regulatory compliance.
- SSAE16 attestations for hosted solutions.
- Continual business process improvement for operational efficiency and quality improvement.

After further inquiry and discussions with the Organization's Senior Vice President of Operations, the IT Examiners noted that there is no formal Internal Audit function at AAIS. The "Internal Audit Program" referred to by AAIS in its response noted above is more of a peer review process, with the areas to be reviewed being selected by the Vice President responsible for a particular functional area.

An external audit of actuarial services was performed in October, 2013 by Pinnacle Actuarial Services. Recommendations included in Pinnacle's August, 2015 report are being incorporated into ongoing operations. An SSAE 16 SOC2 engagement was initiated with Linford and Co. on June 29, 2015, for the AAIS Underwriting Platform. ***As neither of these constitutes an internal audit function, we determined that the internal audit function at AAIS is not formally defined and is not a "true" internal audit function (e.g., an independent and objective function, as described by the Institute of Internal Auditors guidance).***

Recommendations: Management should consider implementing an independent (or semi-independent) function to perform periodic reviews. Depending on cost-benefit considerations, an independent internal audit function reporting to the Board of Directors ("BOD") may be appropriate. If deemed too expensive or impractical for AAIS' size/scope, another consideration could be implementing reviews that could be done as part of the "second line of defense" from a risk management perspective.

AAIS Response: AAIS states that most areas of the organization have external audits. Further, BOD action is set to appoint an internal auditor. This accounting function at AAIS reports directly to the CEO and to the Audit Committee of the BOD.

Standard 13 - The advisory organization has appropriate controls, safeguards and procedures for protecting the integrity of computer information.

Results: Standard Met

Observations: The IT structure at AAIS is organized in a non-hierarchical manner with the Senior Vice President of Operations having overall responsibility for Information Technology. Eight functional areas were

identified with unique technology requirements and support services. The functional areas are organized into three "Technical Centers" under the direction of a member of senior management. From a functional IT perspective, the IT Infrastructure resources are organized under the Senior VP of Operations, while the development resources report into the Vice President of Membership Engagement (who reports to the Senior Vice President of Operations) and the data processing resources report to the VP of Data Engineering who reports to the Chief Actuary. Therefore, the IT department is not truly independent of the operating units for which it performs data processing functions. The development resources are organized under the VP-Membership Engagement and support the customer-facing applications. Also, the Data Engineering group report to the Vice President - Chief Actuary who also manages the main users of the stat data. However, functions within the IT department (development vs. operations) are segregated.

Facility access is restricted through the use of key cards. AAIS employees must swipe the keycard at the door in order to access the office facility. If the employee does not swipe their keycard, an alarm will sound when the employee swipes to exit the facility. In addition to the keycards, the access points are monitored by video surveillance.

AAIS leverages Amazon Web Services Virtual Private Cloud (AWS VPC) infrastructure to support the production servers. Physical access to the Amazon AWS servers is the responsibility of Amazon. On an annual basis, a SOC report is provided by Amazon which attests to the controls in its environment. The IT Examination team requested that the Company provide evidence of the SOC report for AWS. The IT Examiners obtained a copy of the most recent report and confirmed that it addressed the controls in place during the Period. The IT Examiners also noted that the report does not contain any complementary user controls; therefore, AAIS would not have to perform any additional activities to place reliance on the controls. However, there is no evidence that management has reviewed the reports to assess any control exceptions/failures.

In addition to the servers at AWS, there is a small computer room located on-site in Chicago, IL with servers for performance purposes. The building management company for the location uses a temperature monitoring system; however, the room is absent any smoke detectors. ***It appears that the computer/communication facilities (e.g., computer room, network operations center, wiring closets, etc.) are secure and protected from hazards. In addition, access to the computer/communication facilities is restricted to only authorized personnel at all times.***

AAIS employs a *"defense in depth"* strategy to protect its network. An Incident Response plan has been developed to address cybersecurity threats; however, the plan has never been initiated (i.e. AAIS has never had an incident which would require them to execute the plan). A combination of firewalls, filtering (network and desktop), and monitoring tools helps to ensure a secure environment.

AAIS uses a firewall to restrict inbound and outbound traffic on the AAIS corporate network. The rules in place on the firewall have been established to restrict the types of allowable traffic to only those necessary to communicate with the Organization's clients and to conduct AAIS business. Firewall rule sets are configured to block unauthorized public Internet access to AAIS systems. Firewall device configuration is restricted to authorized individuals only through the ACLs and rule sets of each network device. Qualys is used to perform internal

penetration testing on a periodic basis. ***Based on the testing performed, AAIS uses firewall technology to protect its internal network from unauthorized external access.***

Data encryption has not been implemented for *"data at rest;"* however, encryption is available for external email communication via "Message Center" software. Transmission of data between AAIS clients and their production instances is performed through web browsers.

Hypertext Transfer Protocol Secure ("HTTPS") is the method used to transmit the data securely between AAIS clients and the Organization. Data transmissions are encrypted using Transport Layer Security ("TLS") over HTTP with digital certificates issued by a recognized third-party provider. Transport Layer Security is a cryptographic protocol that provides secure communications on the Internet for such things as web browsing, email, Internet faxing, instant messaging and data transfers to web applications. Through the use of TLS over an HTTP, all connections between AAIS's clients and its Underwriting Platform are secured using industry standard encryption. ***It appears the Organization has the proper protocols in place to ensure information is securely transmitted across the Internet.***

AAIS has automated email filtering to scan for dangerous file types such as executable files and scripts. Messages with dangerous files are automatically moved to a quarantined location for review and analysis. AAIS provided screenshots to the IT examiners of its automated solution for scanning email attachments. ***Based on the settings noted in the screenshots, the Organization appears to be properly scanning all incoming email for malicious content.***

The Organization uses Active Directory for authentication and VPN access. Access is controlled according to AAIS policy, and access to the applications and underlying infrastructure is restricted only to authorized individuals. When employees are hired (on-boarded), a new hire checklist is completed that identifies the system access an employee requires. All modifications to user access on the Underwriting Platform and underlying infrastructure must be approved by a Supervisor or Human Resources ("HR") representative. When users terminate employment with the Organization, Human Resources notifies the IT department to deactivate the terminated user IDs.

To help ensure that privileged account access is appropriate, AAIS performs annual entitlement reviews and removes unauthorized user accounts as needed. HR maintains a spreadsheet of access for each user which is emailed to management for review and approval. The process is tracked in Rally. Any changes/updates are communicated to IT for further action; however, the Examiners recommend that the process for performing the annual user access review should be revised. Currently, as previously commented, user access is tracked in spreadsheets which are maintained by HR and reviewed by relevant management personnel. Updates to the spreadsheets are made based upon access requests; however, these spreadsheets may not be an accurate reflection of the current production environment, the result of which means that managers may not be approving the actual level of access that has been granted to each user.

Login to Linux servers is facilitated using a private key. The key management process is performed by the end users. Users authenticate to the Windows Active Directory which grants them access to the network and the associated resources. Users are required to provide a unique username and password in order to

authenticate. AAIS has established a policy which describes the Organization's requirements for acceptable password selection and maintenance.

- Passwords much be changed every 90 days.
- Passwords should be difficult to guess and include uppercase, lowercase, special (e.g., punctuation and extended character set), and numeric characters. They should not include dictionary words or names.
- Password Rules
    - Passwords must be 9 or more characters in length.
    - Cannot contain username.
    - Must include at least three of the following:
        - Uppercase letter
        - Lowercase letter
        - Numeral
        - Special character
    - Cannot match 15 previous passwords.

Remote access is permitted via a VPN which authenticates against the Active Directory. Based on information gathered during a walkthrough, the IT Examiners requested additional details regarding AAIS' IT password processes. The Organization provided a copy of its Information Security Policy. The IT Examiners noted that all Electronic Resources that store AAIS information, or that are permanently or intermittently connected to internal computer networks, must have a password-based access control system approved by EIS. In addition, we noted that in order to appropriately secure access to AAIS's electronic resources, users must follow acceptable password management protocols. In addition, AAIS provided the following policies:

- Information Security policy
- Password Policy
- VPN Remote Access Policy

The IT Examiners reviewed the Organization's policies and noted they are written from an end-user perspective and not truly organizational policies; however, they do specify the password policy and also confirm that remote access utilized authentication via Active Directory.

The IT Examiners noted that leverage would be provided from the SOC reporting for the Underwriting Platform performed by the External Auditors, Linford and Co. The IT Examiners reviewed a copy of the most recent SOC report and were able to identify control testing which addressed the password parameters.

The explanations and documentation provided suggest access to the advisory organization's network and computer systems is minimally protected with user IDs and passwords, based upon the sensitivity of the information and the requirements of the individuals.

Antivirus software is installed on all AAIS workstations with access to the network infrastructure. All workstations update automatically using automated update processes. Virus update engines and data files

are monitored by staff who are responsible for keeping all virus patterns up-to-date. New versions of anti-virus software are pushed to workstations within one week unless there is a valid reason not to push the updates. Symantec virus protection is installed on all laptops and windows servers. Email alerts generated from the virus protection are received by IT and investigated. Macintosh computers use BitDefender; however, updates need to be performed manually by the end users.

AAIS personnel monitor the connectivity to the applications/infrastructure on a 24/7 basis. Security Incidents are initially handled by Amazon and firewall alerts go to the Network Admin. For each AAIS system, the Organization maintains a mailing list of who to notify if an alert is triggered. AAIS uses graphical monitoring tools that provide an historical representation of gathered statistical data. Specifically, application connectivity, response times, Input/Output volume, database connections and read latency are monitored on a continuous basis using active monitoring systems. AAIS also uses tools to monitor CPU, memory and disk usage. These tools help ensure that system resources are not only functioning but are also available to clients. AAIS utilized the following monitoring tools:

- An Event Log is maintained in Confluence which details any security incidents. This is mostly for customer service purposes.
- ICINGA is used for network monitoring purposes. Email alerts are sent to the IT group for triage and resolution.
- Graylog is used for log file aggregation and analysis. This is detective only.

The Organization's systems are configured to notify system administrators via an alert in the event certain system performance and availability threshold metrics are met in accordance with service level agreements. This allows for a proactive response immediately to any potential issues with network and system resources. For alerts that need to be addressed, a defect or ticket will be created and addressed with AAIS personnel in a timely manner. ManageEngine is used to track help desk requests and incident management. Requests are also received via email/cellphone. The IT Examiners noted that AAIS' IT activities are not consistently tracked in the same place using the same technology, based on responses received from the Organization. For example, some significant tasks are tracked in Rally whereas others are haphazardly tracked in ManageEngine. This lack of consistency may increase the risk of the Organization's IT activities not being handled in the same manner or reported consistently for future tracking purposes.

The ITGC environment at AAIS consists of a mix of operating systems including Windows and Linux and between 15 and 20 applications. The applications are a mix of vendor-maintained, vendor maintained (i.e. third-party) and in-house developed; however, a unified process is followed to manage changes to the applications. The majority of the in-scope applications are managed by third-party vendors who are responsible for changes to their applications, databases, etc. Changes to in-house applications, databases, etc. are managed using Rally and include IT services being hosted in the cloud by Amazon. Changes are initiated for a variety of reasons including:

- changes to regulatory requirements,
- technology changes, and
- issues with the applications.

Changes are authorized, designed, developed, configured, documented, tested, approved and implemented in accordance with the Organization's security requirements. To ensure a consistent process for making changes is followed, AAIS has created documented policies and procedures that describe the requirements for making changes to information systems. The policies and procedures are in place to ensure security commitments and requirements are addressed during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification and maintenance of system components. The intent of the change management documentation is to create an effective framework that provides consistency, continuous oversight, approval processes and history of changes that occur. The scope of the documentation covers the change management processes for AAIS' IT infrastructure, installed software and application development. The IT Examiners noted that leverage would be provided from the SOC reporting for the Underwriting Platform performed by external auditors, Linford and Co. The IT Examiners reviewed a copy of the most recent SOC report and identified control testing relevant to this Control Objective. ***The IT Examiners noted that changes to the application portfolio appear to be authorized, controlled and documented.***

Depending on the type of change request, AAIS will either submit a defect to the vendor for a "fix" to be included in a future release or request authorization to begin a change internally. For authorized changes, a member of the development team makes the required change in his or her local development environment, tests the change locally and then commits the change back to the central repository. Following successful unit testing, developers will deploy code to the development acceptance server where integration testing is performed through an automated tool called Selenium. In addition to automated Quality Assurance ("QA") testing within Selenium, all significant system functionality is manually tested by a Product Analyst prior to each release. Any issues found are documented and tracked in the development tracking system as a defect for remediation. Between these two testing methods, the entire production code base is tested at least once manually and many times programmatically prior to every release, regardless of the number of changes made. ***Based on the testing performed, the IT Examiners noted that computer programs/databases/files impacted by user change requests appear to be properly monitored, modified, tested and migrated to the secure production libraries.***

Leveraging the AAIS deployment infrastructure, most deployments can be made without downtime or even interrupting current users' sessions. Access to push changes into the production system is limited to authorized AAIS development team members. Changes are approved for implementation within the release tracking spreadsheet and implemented into production. GIT is used as the source code management tool for application changes. Perforce Commons is used to maintain the code for the actuarial applications and spreadsheets. Jenkins is used for build management and contains the jobs to migrate changes to production. ***Based on the results of testing, the IT Examiners noted that user departments review, approve and sign-off on the implemented changes and the test results prior to the migration to the production environment and there are sufficient controls in the migration of the new application components to the production environment which guarantee accuracy and completeness.***

Recommendations:

- Management should consider using ManageEngine to track all IT tasks and using Rally to document development efforts and significant project management aspects. This will remove potential "noise" from Rally and allow the Company to quickly identify strategic, high-priority tasks.
- Management has begun a process of implementing a consistent end-point solution across all platforms. Management should continue the implementation of virus protection software across all company computers which connect to a central authority on a scheduled basis to update virus definitions. This process will help minimize the risks for malware, ransomware, etc.
- Management should update the access review process to reconcile the user access as stated in the spreadsheets with the current production environment (i.e., the actual access granted to personnel) prior to distributing the spreadsheets for manager review and approval. While the access for some systems may not change often, the periodic review acts as a compensating control for the access provisioning process. The access should not be based on what the end-users feel is needed for them to perform their job functions, but rather should be based on appropriate levels of role-based access for the users' job function/responsibilities.
- AAIS should consider reorganizing the IT department under a single entity which is independent of the processing units. This would involve realigning the data engineering functions under IT and removing them from their respective business units.
    - AAIS Response: AAIS believes its decentralized IT function, while not orthodox, best suits its operations and structure.
- Management should formally document the review of any SOC reports for third-party providers (such as AWS). Amazon Web Services is listed as a sub-service provider in the SOC report for the Underwriting Platform and is carved out of the report. The AWS SOC report may identify issues at AWS which would need to be evaluated to understand any potential effect on AAIS' control environment. The review needs to be formally documented and retained.

Standard 14 – The advisory organization has a valid disaster recovery plan.

Results: Standard Met

Observations: The IT Examiners reviewed documentation to ensure that critical business applications, databases and files are regularly backed up and stored off-site. Disaster recovery (DR) is a key component of business continuity and the Organization's DR Plan describes the steps AAIS will take when the Organization is unable operate in a normal environment, resulting from a natural or man-made disaster. The focus of the DR Plan is to restore the systems that support critical business functions to enable the Organization to return to normal operations as soon as possible with little or no impact to the customer. Tests of business continuity since the move to AAIS's new office location confirmed that the new technology enables AAIS staff to work remotely for an indefinite period of time.

Data backups are performed on a daily basis to a virtual tape library. Production data is backed up on a nightly basis. Production servers are backed up on a more frequent basis (approximately every 4 hours). The data at Amazon is replicated from its east coast facility to the west coast facility on a nightly basis. The IT Examiners requested the following:

- Screenshot showing the schedule for backup of data
- Copy of the backup log showing the success or failure of the nightly backup

The IT Examiners reviewed the Organization's response and noted the server backups are scheduled to occur on a daily basis and are successfully completed. Given the AAIS infrastructure is located at AWS, the backups are stored off-site by default. The IT Examiners reviewed the SOC report for AWS and noted "AWSCA-10.2: Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones." which was tested by the IT examiner with no exceptions noted.

Based on a review of the information provided, it appears the Organization ensures its data is routinely backed up and replicated off-site.

A DR plan exists, which addresses how a disaster is declared and the procedures to recover the IT environment. Disaster Recovery/Business Continuity Plans exists in Confluence which is a vendor-hosted system. Therefore, the plans are stored offsite by default. As the production servers sit at either Amazon or vendor locations, the practicality of performing an actual DR test is questionable. However, a tabletop exercise would be recommended annually. To further evaluate the Organization's disaster recovery process, the IT Examiners requested the following information:

- A copy of the Organization's current DR plan and a summary of the changes since the last examination.
- Screenshot showing the location of the DR policy in Confluence.

The IT Examiners reviewed the Organization's response to the request and noted:

- The business continuity plan clearly describes senior management's roles and responsibilities associated with the declaration of an emergency and implementation of the business continuity and disaster recovery plans.
- The plan clearly identifies the general process by which the threat will be assessed and the specific individuals who are authorized to declare an emergency.

In addition, the IT Examiners reviewed the DR plan and noted **the DR Plan does not:**

- Contain a list of critical statistical agent and ratemaking computer application programs, operating systems and data files.
- 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.
- Assign a restoration priority to all significant statistical agent and ratemaking activities.
- Identify if user departments have developed adequate manual processing procedures for use until the electronic data processing function can be restored.

In addition, the IT Examiners confirmed the last time the DR Plan had been tested was 2 years ago when the Organization moved into its current office facility. ***As such, the Organization does not appear to be properly testing the plans and addressing issues discovered during the testing.***

Recommendations: Management should consolidate their current DR Plan into a single document, which would address all company applications and expand the document to include detailed procedures for recovering all applications in the environment. AAIS' processing environment is located at third-party providers, which removes the likelihood that an issue at an AAIS' physical location would cause a service disruption. However, issues caused by data corruption (whether these issues were caused through normal processing or cyber security related issues, nonetheless resulting in modified data) are not dependent upon the physical location. This situation could result in disaster recovery procedures that need to be implemented to recover the application/environment back to a known-good point in time. In addition, the DR Plan should be tested on an annual basis to confirm that the activities, applications, contacts, etc. are current. Given the location of AAIS' assets at a third-party, a tabletop exercise may be sufficient.

Data Collection and Handling

Standard 1 - The statistical agent's series of edits are sufficient to catch material errors in data submitted by a company.

Results: Standard Met

Observations: The IT Examiners obtained a copy of the current *Statistical Handbook of Data Available to Insurance Regulators* (the "Statistical Handbook") from the NAIC. The version which was downloaded from the NAIC website was dated 2012 and was noted to be the most current version. The IT Examiners reviewed the Handbook and noted the following information:

- The *Statistical Handbook* provides two intertwined sets of requirements – one for insurers, and one for statistical agents. The purpose of these requirements is to provide assurance that reports from statistical agents are acceptably accurate as representations of the insurance written and the losses incurred by insurers.
- Statistical agents are required to apply edits and checks to data received from insurers, and insurers are required to respond to the queries presented by statistical agents. The reporting "requirements" contained in the Statistical Handbook reflect the minimum statistical compilation and report formats recommended by the NAIC's Statistical Information (C) Task Force.

In response to the IT Examiners request for evidence of edits performed for the various data types, AAIS provided documentation detailing the requirements, record layouts, and criteria for each data element in the various reporting statistical plans:

- Agricultural Output Statistical Plan
- Business Owners / Artisans Statistical Plan
- Automotive Statistical Plan

- Boat Owners / Yacht Statistical Plan
- Commercial Properties
- Crime Statistical Plan
- Dwelling Properties and Farm Properties Statistical Plan
- Farm Owners Statistical Plan
- General Liability Statistical Plan
- Glass Statistical Plan
- Homeowners Statistical Plan
- Inland Marine Statistical Plan
- Mobile-Homeowners Statistical Plan

The IT Examiners compared the required data elements from the Statistical Handbook with the data elements specified in the statistical plan documents and confirmed that the documents addressed the required data elements. In addition, the IT Examiners noted that the plan documents also defined the criteria for each data element.

The data received by AAIS for statistical reporting is expected to follow the filed Statistical Plans. The Statistical Plans are based, in part, on the regulations and direction provided by the entities that define the reporting requirements. In order to ensure that as much quality data is processed in a timely manner, the validation rules can be modified to support "in-progress" changes. In addition, AAIS staff can acknowledge and process data that does not meet all validation criteria for report or other processing, at the direction of the affiliate, if the affiliate is unable or unwilling to make the necessary changes to support the new plans.

After reviewing the plan documents, the IT Examiners requested the following:

- Documentation of data edit definitions and validations for various data types.

In response to the request, the Organization provided the data validation matrices for the included statistical plans and documentation of the operation of the SDMA application. The IT Examiners reviewed the SDMA manual and confirmed that it details a high-level description of the validation process. The IT Examiners reviewed the edit matrices and noted that the definitions included both "general" edits and validations and plan-specific edits. The "general" edits include:

- Common – Provides general edits and validations such as data types and date ranges.
- Geography – Provides data edits and validations for geographic fields (e.g., zip code, country code, etc.).

The IT Examiners reviewed the matrices and determined that the edits appeared to be appropriate.

For the plan-specific validations, the IT Examiners leveraged the sample of filings which were selected by the actuary resources on the engagement team. A total of 15 samples were selected by the Actuarial Examiners covering four Statistical Plans: Homeowners, Businessowners, Commercial Properties, Inland Marine, and Farm Owners.

Company Tracking #	Filing Type	Product	Project Name	State
AAIS-2015-24LC	Rate	Homeowners By-Peril	Revised Base Loss Costs	Utah
AAIS-2015-24R	Rule	Homeowners By-Peril	Revised Rules and Factors	Missouri
AAIS-2015-16R	Rule	Businessowners	New & Revised Rules, Supplementary Rating Information, Classifications and Territorial Definitions	Delaware
AAIS-2015-16R	Rule	Businessowners	New & Revised Rules, Supplementary Rating Information, Classifications and Territorial Definitions	South Dakota
AAIS-2015-16R	Rate/Rule	Businessowners	New & Revised Rules, Supplementary Rating Information, Classifications and Territorial Definitions	Wisconsin
AAIS-2015-16R	Rule	Businessowners	New & Revised Rules, Supplementary Rating Information, Classifications and Territorial Definitions	Oklahoma
AAIS-2015-16R	Rate/Rule other than PPA	Businessowners	New & Revised Rules, Supplementary Rating Information, Classifications and Territorial Definitions	Georgia
AAIS-2015-16R	Rule	Businessowners	New & Revised Rules, Supplementary Rating Information, Classifications and Territorial Definitions	Minnesota
AAIS-2015-16LC	Loss Cost	Businessowners	Revised Loss Costs	New Hampshire
AAIS-2015-3R	Rule	TRIA2015	TERRORISM RISK INSURANCE PROGRAM REAUTHORIZATION ACT OF 2015	Massachusetts
AAIS-2015-16LC	Drawer – Lost Cost	Businessowners	Revised Loss Costs	Illinois
AAIS-2013-32LC	Loss Cost	2013 Inland Marine Guide	Revised Loss Costs	Texas
AAIS-2014-37LC	Loss Cost	2014 Personal Inland Marine	Revised Loss Costs	New York
AAIS-2014-77FOR	Loss Cost	2014 Farmowners	Revised Loss Costs	Maryland
AAIS-2015-24LC	Loss Cost	2015 Homeowners By-Peril	Revised Loss Costs	Virginia

Note: The terrorism risk is a filing that affected multiple lines of business, so no specific Statistical Plan was affected by that filing.

The IT Examiners obtained the edit matrices for the Statistical Plans included in the sample and noted that the edits/validation appeared appropriate and in-line with the Statistical Handbook. While only the plans which are included in the sample filings are listed, edits/validations for all applicable statistical plans were reviewed.

The IT Examiners performed a walkthrough of the data editing process using a sample filing. Since the process is automated and all data received through the SDMA is subject to editing, they walked through 1 sample (2015 Homeowners By-Peril – Utah). The IT Examiners obtained screenshots confirming that edits were performed.

Recommendations: None

Standard 2 - All data that is collected pursuant to the statistical plan is run through the editing process.

Results: Standard Met

Observations: Please refer to Standard 1, "The statistical agent's series of edits are sufficient to catch material errors in data submitted by a company." under Data Collection and Handling for relevant testing, as these standards were tested in conjunction with each other. ***Based on the procedures performed, all data that is collected pursuant to the statistical plan is run through the editing process.***

Recommendations: None

Standard 3 - Determine that all databases are updated as needed with all accepted company data.

Results: Standard Met

Observations: In response to the request, the IT Examiners obtained the current copy of the Organization's Analytics Department Procedures. The IT Examiners reviewed the document and noted that the SDMA application allows statistical data to be submitted, validated, corrected and approved through a web browser. It helps streamline the data submission process, provides consistent validation and provides more visibility and control for affiliates into their data, including the ability to make corrections directly online. Once the file is approved, the data is moved to the Data Resource Center ("DRC") where the compliance reports and other analytics are performed.

The IT Examiners also requested and reviewed the following information:

- Copies of the following documents identified in the Data Engineering Department Overview document
    - Statistical Data Collection Policies and Procedures

- Statistical Reporting Policies and Procedures
- DRC Policies and Procedures

The IT Examiners performed a walkthrough of the processes for populating the DRC with the data and confirmed that the DRC is an SAS environment. The IT Examiners obtained screenshots of the process to transfer the data from SDMA to the DRC. The IT Examiners reviewed the data scripts and confirmed the statistical data is transferred from SDMA into the DRC (SAS Environment). In addition, the IT Examiners walked through a data element from the first filing (2015 Homeowners by-Peril – Utah) and confirmed that the data elements are available in the DRC. In addition, per the AAIS response in the CAA document, the IT Examiners noted that AAIS performs checks on data to confirm the data quality is consistent with past experience and possible changes in its affiliates markets. For various reports, they calculate a percent change from prior year to current year. A Tableau report was developed to review Annual Statement data for the percent of deviation between each company by state and line. The IT Examiners obtained a copy of the Tableau report and confirmed that the report is used to monitor the completeness of the data in the Stats data mart. ***Based on the procedures performed, statistical databases appear to be updated as needed with all accepted company data.***

Recommendations: None

Standard 4 - Determine that statistical data is reconciled to the State Page - Exhibit of Premiums and Losses, Statutory Page 14, of the NAIC annual statement on an annual basis.

Results: Standard Met

Observations: The IT Examiners noted in the AAIS response to the CAA that the Organization has created a Tableau application to match received statistical data to NAIC data. The IT Examiners confirmed this report has been in place for approximately 12 months which would align with the end of the examination period. The IT Examiners also confirmed with the Vice President - Data Engineering, that the report was implemented in July 2014. The IT Examiners obtained a copy of the report and noted that the report reconciles the data for premiums to NAIC data. Prior to the implementation of the Tableau report, the IT Examiners noted that AAIS performed a reconciliation of premium/loss data to NAIC data using an analytical spreadsheet. The IT Examiners obtained a copy of the spreadsheet and confirmed the reconciliation of the AAIS data to the NAIC data for Premiums and Losses which is the data on State Page 14. ***Based on the procedures performed, statistical data is reconciled to the State Page - Exhibit of Premiums and Losses, Statutory Page 14, of the NAIC annual statement.***

Recommendations: None

Standard 5 - Determine that all calculations associated with the database have been accurately applied.

Results: Standard Met

Observations: The IT Examiners obtained the current copy of the Analytics Department Procedures from AAIS. The IT Examiners reviewed the document and noted that data processed through the SDMA that has been "accepted" by AAIS or "acknowledged" (i.e., data that may have some errors but has been approved by the affiliate to use for reporting that does not necessarily pass AAIS muster) is moved by data integration programs and procedures to the DRC for use in the reporting process. AAIS' Statistical Reporting staff review reporting requirements from the various entities that AAIS reports to and use the data in the DRC to prepare, validate, and submit reports.

The IT Examiners leveraged the sample of filings which were selected and tested by RRC's Actuarial Examiners. A total of 15 samples were selected by the Actuarial Examiners covering four Statistical Plans: Homeowners, Commercial Properties, Inland Marine, and Farm Owners. As sample 10 covered multiple statistical plans, we excluded that sample from this analysis. The IT Examiners, with the assistance of AAIS resources, walked through selected data elements from the filings and tied them back to the SAS database (DRC). The IT Examiners were able to do this for all sample filings. In addition to the specific data elements, certain calculations were also investigated and determined to be accurate based on recalculation using the validated data elements. ***Based on the procedures performed, AAIS employs data completeness tests as outlined in the NAIC Statistical Handbook of Data Available to Insurance Regulators.***

Recommendations: None

Standard 6 - Where applicable, determine that the statistical agent employs use of data completeness tests as outlined in the NAIC Statistical Handbook of Data Available to Insurance Regulators.

Results: Standard Met

Observations: Please refer to Standard 1, "The statistical agent's series of edits are sufficient to catch material errors in data submitted by a company." under Data Collection and Handling for relevant testing, as these standards were tested in conjunction with each other. ***Based on the procedures performed, AAIS employs data completeness tests as outlined in the NAIC Statistical Handbook of Data Available to Insurance Regulators.***

Recommendations: None

Correspondence with Insurers and States

Standard 1 - The statistical agent keeps track of companies that fail to meet deadlines.

Results: Standard Met

Observations: The IT Examiners obtained the current copy of the Organization's Analytics Department Procedures. The IT Examiners reviewed the document and noted that in order to ensure that quality data is processed in a timely manner, the validation rules in the SDMA can be modified to support "in-progress" changes. In addition, AAIS staff can acknowledge and process data that does not meet all validation criteria

for report or other processing, at the direction of the affiliate, if the affiliate is unable or unwilling to make the necessary changes to support the new plans.

There are a number of formal and informal monitoring and control points throughout the Statistical Data Acquisition process. Salesforce.com and the SDMA are the primary "control" and "monitoring" points for all affiliate communication regarding statistical data. These tools provide an audit trail, the content of the data, output from the validation routines, communication tracking, etc. There are a number of other points during normal operations where these tools are checked to ensure that AAIS is following the appropriate protocols:

- Sprint Planning – every two weeks, AAIS reviews the tasks (in Rally) that are in progress. Statistical Reporting Acquisition is an ongoing process that is discussed at nearly every Sprint Planning meeting.
- A number of the regulatory reports are used to monitor and track the quality and completeness of the data processing. Data in the Statistical Reporting application is compared to data in the Data Mart to ensure that all "accepted" or "acknowledged" data has been made available to the Statistical Reporting Team.

The IT Examiners requested the following:

- Copies of the following identified in the Data Engineering Department Overview document
    - Statistical report tracking in Perforce Commons

The IT Examiners obtained copies of the spreadsheets from 2014 and 2015 which are used to track the Statistical Data calls. We noted that all calls for 2014 and 2015 had been received. In addition, the IT Examiners noted that the 2015 spreadsheet contains a column which maps the stat plan data with the associated Rally task. This provides a linkage to the task tracking in Rally. ***Based on the procedures performed, AAIS keeps track of companies that fail to meet deadlines.***

Recommendations: None

Standard 2 - The statistical agent has established procedures for notifying companies (and regulators, as requested or required) of material errors and for correcting those errors (also reference Standard 2, Operations/Management/Governance).

Results: Standard Met

Observations: The IT Examiners obtained the current copy of the Analytics Department Procedures from AAIS. The IT Examiners reviewed the document and noted: "There are a number of formal and informal monitoring and control points throughout the Statistical Data Acquisition process. Salesforce.com and the SDMA are the primary "control" and "monitoring" points for all affiliate communication regarding statistical data. All "formal" communications – i.e. communications that have reports, approvals, directions, etc. – are tracked in Salesforce.com. This includes voicemail, email, mail, Internet submissions and phone calls."

The IT Examiners obtained samples of conversations from Salesforce.com and confirmed that AAIS maintains communication with its affiliates regarding errors in the data and correcting the errors. In addition, The IT Examiners leveraged the sample of filings which were selected by the actuary resources on the engagement team. A total of 15 samples were selected by the Actuarial Examiners covering four Statistical Plans: Homeowners, Commercial Properties, Inland Marine, and Farm Owners. The IT Examiners, with the assistance of AAIS resources, walked through the sample filings and confirmed the communication of data issues with affiliates. ***Based on the procedures performed, AAIS has established procedures for notifying companies of material errors and for correcting those errors.***

Recommendations: None

Standard 3 - The statistical agent maintains a follow-up procedure with companies that have reporting errors or questions.

Results: Standard Met

Observations: Please refer to Standard 2, "The statistical agent has established procedures for notifying companies (and regulators, as requested or required) of material errors and for correcting those errors" under Correspondence with Insurers and States for relevant testing, as these standards were tested in conjunction with each other. ***Based on the procedures performed, AAIS maintains a follow-up procedure with companies that have reporting errors or questions.***

Recommendations: None

Standard 4 - Review any additional data quality programs maintained by the statistical agent pertaining to data collected pursuant to the statistical plan.

Results: Standard Met

Observations: The IT Examiners noted in the AAIS response in the CAA document that AAIS has implemented a formal data governance process in 2013 which includes procedures for insuring data quality. This data governance process has been implemented as part of the Statistical Reporting Data Mart which has automated data quality testing and reporting. While the primary process for ensuring data quality is the SDMA process described above, as part of the overall IT Governance structure, AAIS has implemented an IT Strategic Planning Governance Committee, Application Governance Committee and a Data Governance Committee. The IT Examiners confirmed with the Senior Vice President - Operations and corroborated with by the Vice President - Data Engineering that minutes of the meetings are maintained in Rally.

Additionally, the IT Examiners noted that affiliate data that does not meet minimal quality requirements is excluded from the statistical reporting process. The NAIC is informed of any affiliate's data which is excluded from the reporting process. The IT Examiners obtained a copy of communication with the NAIC informing them that an affiliate's data will be excluded from the data reported by AAIS. ***Based on the procedures performed, AAIS performs additional data quality activities beyond the validations in the SDMA.***

Recommendations: None

Standard 5 - With each standard premium and loss report to the states, the statistical agent provides a listing of companies whose data is included in the compilations and a historical report listing.

Results: Standard Met

Observations: Please refer to Standard 4, "Review any additional data quality programs maintained by the statistical agent pertaining to data collected pursuant to the statistical plan." under Correspondence with Insurers and States for relevant testing, as these standards were tested in conjunction with each other. ***Based on the procedures performed, AAIS provides a listing of companies whose data is included in the compilations and a historical report listing.***

Recommendations: None

Reports, Report Systems and Other Data Requests

Standard 1 - All calculations used to develop the database have been performed accurately.

Results: Standard Met

Observations: The IT Examiners obtained the current copy of the Organization's Analytics Department Procedures. The IT Examiners reviewed the document and noted: "Data processed through the SDMA that has been "accepted" by AAIS or "acknowledged" (data that may have some errors but has been approved by the affiliate to use for reporting that does not necessarily pass AAIS muster) is transferred by data integration programs and procedures to AAIS's DRC for use in the reporting process. The Statistical Reporting staff review reporting requirements from the various entities that AAIS reports to and use the data in the DRC to prepare, validate, and submit reports.

The IT Examiners leveraged the sample of filings which were selected by RRC's Actuarial Examiners. A total of 15 samples were selected by the Actuarial Examiners covering four Statistical Plans: Homeowners, Commercial Properties, Inland Marine, and Farm Owners. The IT Examiners, with the assistance of AAIS resources, walked through selected data elements from the filings and tied them back to the SAS database (DRC). The IT Examiners were able to complete this for all sample filings. In addition to the specific data elements, certain calculations were also investigated and determined to be accurate based on recalculation using the validated data elements.

The IT Examiners noted in the AAIS response in the CAA that in addition to the rules-based quality checks performed by the SMDA, actuarial staff perform data quality checks, including peer review, on the data selected for a data analysis. The IT Examiners confirmed with the Senior Vice President - Operations and corroborated with by the Vice President - Data Engineering that the data is reviewed by the analytics department and peer reviews of the actuarial work are also performed. ***We reviewed selected calculated values for the sampled filings and confirmed that the calculated values in the reports were accurate.***

Recommendations: None

Standard 2 - The statistical agent has accurately extracted the appropriate information from the statistical database.

Results: Standard Met

Observations: Please refer to Standard 1, "All calculations used to develop the database have been performed accurately." under Reports, Report Systems and Other Data Requests for relevant testing, as these standards were tested in conjunction with each other. ***We reviewed selected data values for the sampled filings and confirmed that the values in the reports were extracted accurately.***

Recommendations: None

Standard 3 - The statistical agent has accurately extracted the appropriate information from the statistical database.

Results: Standard Met

Observations: Please refer to Standard 1, "All calculations used to develop the database have been performed accurately." under Reports, Report Systems and Other Data Requests for relevant testing, as these standards were tested in conjunction with each other. ***We reviewed selected data values for the sampled filings and confirmed that the values in the reports were reviewed based on data from the company.***

Recommendations: None

Standard 4 - Data collected, in addition to the data collected under the statistical plan, was adequately reviewed for quality and compiled according to applicable statutes, rules and regulations.

Results: Standard Met

Observations: The IT Examiners noted in the AAIS response in the CAA that the Organization has a defined ongoing process for reviewing statistical reporting rules, regulations, report specifications, and other statistical reporting information developed by State DOIs as well as related organizations such as the NAIC. The Analytics Services department works closely with the GLC department to ensure that AAIS receives the appropriate specifications, schedules, changes, bulletins, and contacts from all the State Departments of Insurance. The IT Examiners obtained a copy of the tracking sheet for the GLC research and confirmed that data collected under the statistical plan was adequately reviewed for quality and compiled according to applicable statutes, rules and regulations. ***Based on the review of the Statute Reconciliation, data collected was adequately reviewed for quality and compiled according to applicable statutes, rules and regulations.***

Recommendations: None

VII. EXAMINATION SUMMARY

In addition to the General Conclusions and Observations included on pages 6-9 of the Report, the following are specific observations made as a result of the Examination:

Listing of Findings and Recommendations

SCOPE AREA	FINDINGS	RECOMMENDATIONS
ACTUARIAL		
1.	AAIS has significantly improved its actuarial operations since the prior examination, with the addition of credentialed actuaries and the implementation of a peer review process.	Continued focus on AAIS' infrastructure and operations to enhance internal controls and address matters identified during the current examination.
2.	AAIS's loss cost filings lack sufficient documentation.	AAIS should improve the documentation in its loss cost filings so that the basis for the results can be clearly followed by those reviewing the analysis.
3.	AAIS currently targets loss cost filing updates for each line of business within five years. Comparable organizations produce loss cost filings annually.	AAIS should seek to increase the frequency with which it can produce loss cost filings for each line of business. This could be accomplished through a combination of hiring and streamlined data processes.
4.	AAIS's process for preparing and validating data used in loss cost filing reviews is time-consuming and manually intensive.	AAIS should seek to streamline the data processing aspect of its loss cost filing reviews. The Statistical Data Management Application, partially implemented subsequent to the examination period, is expected to help mitigate this issue for AAIS, but other measures should be considered as well, such as penalties for companies that do not submit accurate data.
5.	AAIS implemented a peer review process during the examination period. Documentation of peer review appears to be decentralized, consisting of numerous documents and emails.	AAIS should implement a procedure to centralize and standardize peer review documentation.
6.	AAIS does not appear to include actuarial support for the introduction of new risk classifications and changes to existing risk classifications in its loss cost filings. AAIS does appear to have the actuarial support for such changes, but the documentation appears to be decentralized.	AAIS should include the actuarial support for the introduction of new risk classifications or changes to existing risk classifications in the loss cost filings.

SCOPE AREA	FINDINGS	RECOMMENDATIONS
7.	AAIS includes a provision for Loss Adjustment Expenses in its loss cost filings that is based on industry data, from Best's Averages and Aggregates.	AAIS should consider basing estimates of Loss Adjustment Expenses from its affiliate data rather than industry totals from Best's Averages and Aggregates.
8.	AAIS uses five years of historical experience in all of the loss cost filings reviewed by the examination team.	AAIS should consider varying the number of years used in the loss cost filing depending on the amount of data available for the business included in the analysis.
9.	AAIS considers incurred loss development methods only in its projections of ultimate losses.	AAIS should consider using additional methodologies, such as paid loss-based methodologies.
INFORMATION TECHNOLOGY ("IT")		
1.	AAIS has re-architected and rebuilt its IT infrastructure in order to improve the accuracy and reliability of its IT operations since the prior 2012 examination. These improvements include: • Replacement of the antiquated AS/400 platform with current technology and the implementation of Agile (see below) methodology for operations management. • AAIS improved its Disaster Recovery posture by implementing a cloud-based environment located in a state-of-the-art datacenter which is maintained by an independent third party. • AAIS improved its network infrastructure through the implementation of a Cisco Security Plus Firewall which is monitored and generates alerts based on configured thresholds. • AAIS improved its change management process through the implementation of Source Code management and Release Management utilities and the integration of those utilities into its processes.	AAIS should continue to focus on maturing their infrastructure and enhancing internal controls. AAIS should continue to mature their processes so that these processes are consistently followed, logically organized and complete documentation is retained.

SCOPE AREA	FINDINGS	RECOMMENDATIONS
2.	The IT department is not truly independent of the operating units for which it performs data processing functions. The Data Engineering group is under the VP-Chief Actuary who also manages the main users of the stat data. However, functions within the IT department (development vs. operations) are segregated; therefore, this is considered an observation.	AAIS should consider reorganizing the IT department under a single entity which is independent of the processing units. This would involve realigning the data engineering function under IT and removing them from their respective business units. AAIS should also consider consolidating IT policies and procedures into a unified document.
3.	The process for performing the annual user access review needs to be reworked. Currently, user access is tracked in spreadsheets which are maintained by HR and reviewed by relevant management personnel. Updates to the spreadsheets are made based upon access requests; however, these spreadsheets may not be an accurate reflection of the current production environment, the result of which means that managers may not be approving the actual level of access that has been granted to each user.	Management should update the access review process to reconcile the user access as stated in the spreadsheets with the current production environment (i.e., the actual access granted to personnel) prior to distributing the spreadsheets for manager review and approval. While the access for some system may not change often, the periodic review acts as a compensating control for the access provisioning process. The access should not be based on what the end-users feel is needed for them to perform their job functions, but rather should be based on appropriate levels of role-based access for the users' job function/responsibilities.
4.	Currently AAIS does not employ a consistent, independent function to provide quality control checks and balances (e.g., an Internal Auditor or internal audit-like function). Peer reviews are performed on a periodic basis based on risk areas that are self-identified by management; however, there is no other means currently to identify areas that could benefit from a more formal review.	Management should consider implementing an independent (or semi-independent) function to perform periodic reviews. Depending on cost-benefit considerations, an independent Internal Audit function reporting to the Board of Directors ("BOD") could be appropriate. If deemed too expensive or impractical for AAIS's size/scope, another consideration could be implementing reviews that could be done as part of the "second line of defense" from a risk management perspective.
5.	IT activities are not consistently tracked in the same place using the same technology. For example, some significant tasks are tracked in Rally (part of Agile), whereas others are tracked in ManageEngine. This lack of consistency could increase the risk of IT activities not being handled in the same manner or reported consistently for future tracking purposes.	Management should consider using ManageEngine to track all IT tasks and using Rally to document development efforts and significant project management aspects. This will remove potential "noise" from Rally and allow the Company to quickly identify strategic, high-priority tasks.

SCOPE AREA	FINDINGS	RECOMMENDATIONS
6.	As of 2015, virus definitions for Apple Macintosh computers are dependent upon the user initiating any updates.	Management has begun a process of implementing a consistent end-point solution across all platforms. Management should continue the implementation of virus protection software across all company computers which connects to a central authority on a scheduled basis to update virus definitions. This process will help minimize the risks for malware, ransomware, etc.
7.	The DR plan does not contain sufficient detail to facilitate the timely restoration of processing for an application(s) on a consistent basis and testing of the DR plan is not performed on a consistent basis.	Management should develop the DR plan to be a single document covering all company applications and expand the document to include detailed procedures for recovering all applications in the environment. AAIS' processing environment is located at third-party providers, which removes the likelihood that an issue at AAIS' physical location would cause a service disruption. However, issues caused by data corruption (whether these issues were caused through normal processing or cyber security related issues, nonetheless resulting in modified data) are not dependent upon the physical location. This situation could result in disaster recovery procedures that need to be implemented to recover the application/ environment back to a known-good point in time. In addition, the plan should be tested on an annual basis to confirm that the activities, applications, contacts, etc. are current. Given the location of AAIS' assets at a third-party, a tabletop exercise may be sufficient.
8.	There is documentation to confirm management reviews the SOC report for AWS or adequately monitors the activities of the contracted entity.	Management should formally document the review of any SOC reports for third-party providers (such as AWS). Amazon Web Services is listed as a sub-service provider in the SOC report for the Underwriting Platform and is carved out of the report. The AWS SOC report may identify issues at AWS which would need to be evaluated to understand any potential effect on AAIS' control environment. The review needs to be formally documented and retained.
MARKET CONDUCT		
1.	AAIS has improved the scope and level of documentation related to their practices and procedures since the prior examination.	AAIS should ensure that the Organization adapts a consistent standard for documenting information that addresses all practices and procedures and internal controls.

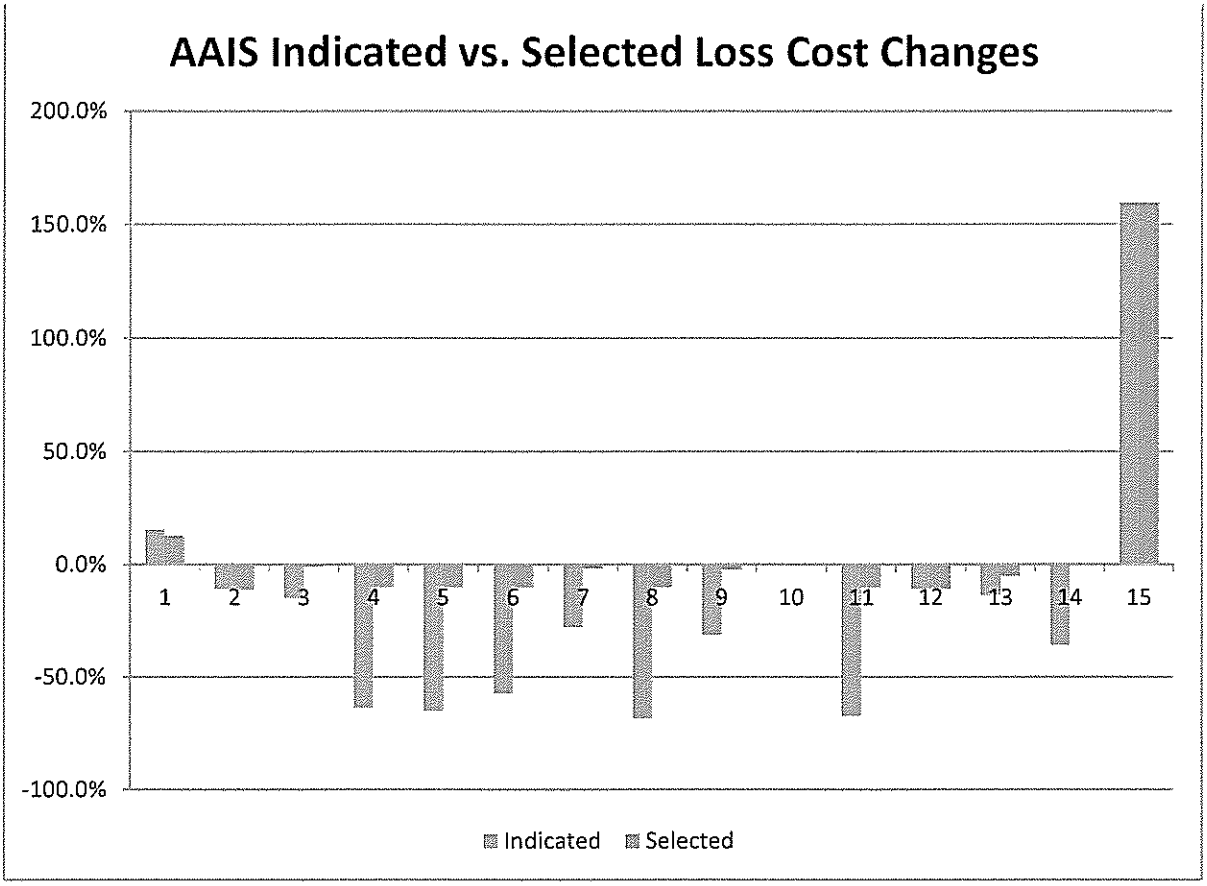
APPENDIX I – LOSS COST/RATE FILING TESTING ATTRIBUTES

Actuarial Standard of Practice	AAIS Sample Loss Cost Filings - Actuarial Testing Attributes	COMMENTS
ASOP #13: Trending Procedures	Actuary should identify intended purpose of trending procedure	The intended purpose is not described in the loss cost filings
	Actuary should select data appropriate for the trends being analyzed	Pass
	Actuary should consider economic and social influences in trend selection	Not included in the loss cost filings, though included in peer review
	Actuary should select trend procedures based on analysis of available data	Pass
	Actuary should consider length of experience and forecast periods in selecting trend period	Not included in the loss cost filings, though included in peer review
	Actuary should evaluate results of trending procedure for reasonableness	Not included in the loss cost filings, though included in peer review
ASOP #23: Data Quality	Actuary should select data that are appropriate for intended use	Pass
	Actuary should check reasonableness and comprehensiveness of data elements	Not included in the loss cost filings, though included in peer review
	Actuary should check data for any known material limitation	Not included in the loss cost filings, though included in peer review
	Actuary should consider the cost and feasibility of obtaining alternate data	Pass
	Actuary should consider benefit to be gained from an alternative data set	Loss adjustment expense assumptions are based on aggregate industry data rather than AAIS's client information.
	Actuary should consider the sampling methods used to collect the data if applicable	Pass
	Actuary may rely on data supplied by others and disclose such reliance	Pass
ASOP #25: Credibility	Actuary should select credibility procedures that are reasonable	Credibility is assigned to state, region, and countrywide experience. No support is provided for the credibility standards.
	Actuary should select credibility procedures that do not tend to materially bias the data	Credibility is assigned to state, region, and countrywide experience. No support is provided for the credibility standards.
	Actuary should select credibility procedures that are practical to implement	Pass
	Actuary should select credibility procedures that balance responsiveness and stability	Many of the loss cost filings indicated large loss cost increases or decreases, suggesting that the experience data may be receiving more credibility than is merited.
	Actuary should use care in selecting the related experience	Pass
	Credibility procedure requires actuary to use informed judgment.	Pass
	Actuary should consider the homogeneity of the subject and related experience for credibility procedures	Credibility is assigned to state, region, and countrywide

		experience. No support is provided for the credibility standards.
ASOP #29: Expense Provisions	Actuary should determine the provisions for loss adjustment expenses; commission and brokerage fees, other acquisition expenses, general administrative expenses and taxes, licenses and fees.	Pass
ASOP #38: Use of Outside Models	Actuary should have a basic understanding of the model	Pass
	Actuary should evaluate whether the model is appropriate for the intended application	Pass
	Actuary should determine that appropriate validation of the model has occurred	Pass
	Actuary should determine the appropriate use of the model	Pass
	Actuary may rely on model evaluation by another actuary	Pass
ASOP #39: Catastrophes	Actuary should identify perils or events with potential for catastrophe losses	Pass
	Actuary should identify, if possible, catastrophe losses in historical insurance data	Pass
	Actuary may use insurance and non-insurance data to determine a catastrophe provision	Pass
	Actuary should evaluate the extent the insurance data are representative of the peril or event identified	Pass
	Actuary should consider applicability of the insurance data to the coverage	Pass
	Actuary should make adjustment to insurance data to reflect future conditions	Pass
	Actuary should consider sensitivity to outcomes if other insurance data would be used	Pass
	Actuary should consider appropriate trend for catastrophes	Pass
	Actuary should make sure that a consistent definition of catastrophe has been used for the data	Pass
	Actuary should ensure that form and content of communication are appropriate to circumstances	Pass
ASOP #41: Communications	Actuary should ensure that communications are clear	*Overall results are not always clear in the exhibits. The sources for assumptions and results are not always provided, as with credibility assumptions.*
	Actuary should ensure that communications are timely	Pass
	Actuarial communication should clearly identify the actuary responsible for it	Not included in loss cost filings
	Actuary should complete actuarial report if findings are to be relied upon by another user	Pass
	Actuarial report should clearly state findings and identify methods, procedures and assumptions	Pass
	Actuary should identify content that is not included in the report	Pass
	Actuarial report should include possible uncertainty or risk in any of the results	Not included in loss cost filings
	Actuarial report should state the reliance on other sources of data or information	Pass

	Actuarial report should identify the party responsible for each material assumption and method	Not included in loss cost filings
ASOP #41: ***Continued***	Actuarial report should identify the dates of the data or other information used in the report	Not included in loss cost filings
	Actuary should disclose any relevant subsequent events where appropriate	N/A
	Actuary should explain any material difference in results of prior reports on the same issue	N/A

APPENDIX II – LOSS COST/RATE FILING TESTING SUMMARIES



Sample	State	Line of Business	Filing Designation
LC Filing 01	Utah	Homeowners	AAIS-2015-24LC
LC Filing 02	Missouri	Homeowners	AAIS-2015-24R
LC Filing 03	Delaware	Businessowners	AAIS-2015-16R
LC Filing 04	South Dakota	Businessowners	AAIS-2015-16R
LC Filing 05	Wisconsin	Businessowners	AAIS-2015-16R
LC Filing 06	Oklahoma	Businessowners	AAIS-2015-16R
LC Filing 07	Georgia	Businessowners	AAIS-2015-16R
LC Filing 08	Minnesota	Businessowners	AAIS-2015-16R
LC Filing 09	New Hampshire	Businessowners	AAIS-2015-16LC
LC Filing 10	Massachusetts	Terrorism Risk Insurance (TRIA)	AAIS-2015-3R
LC Filing 11	Illinois	Businessowners	AAIS-2015-16LC
LC Filing 12	Virginia	Homeowners	AAIS-2015-24LC

STATE OF New Jersey)
) ss
COUNTY OF Monmouth)

Barry L Wells, being first duly sworn upon his/her oath, deposes and says:

That he was appointed by the Director of Insurance of the State of Illinois (the "Director") as Examiner-In-Charge to examine the insurance business and affairs of American Association of Insurance Services (the "Company").

That the Examiner-In-Charge was directed to make a full and true report to the Director of the examination with a full statement of the condition and operation of the business and affairs of the Company with any other information as shall in the opinion of the Examiner-In-Charge be requisite to furnish the Director with a statement of the condition and operation of the Company's business and affairs and the manner in which the Company conducts its business;

That neither the Examiner-In-Charge nor any other persons so designated nor any members of their immediate families is an officer of, connected with, or financially interested in the Company nor any of the Company's affiliates other than as a policyholder or claimant under a policy or as an owner of shares in a regulated diversified investment company, and that neither the Examiner-In-Charge nor any other persons so designated nor any members of their immediate families is financially interested in any other corporation or person affected by the examination;

That an examination was made of the affairs of the Company pursuant to the authority vested in the Examiner-In-Charge by the Director of Insurance of the State of Illinois;

That she/he was the Examiner-in-Charge of said examination and the attached report of examination is a full and true statement of the condition and operation of the insurance business and affairs of the Company for the period covered by the Report as determined by the examiners;

That the Report contains only facts ascertained from the books, papers, records, or documents, and other evidence obtained by investigation and examined or ascertained from the testimony of officers or agents or other persons examined under oath concerning the business, affairs, conduct, and performance of the Company.

Examiner-In-Charge

Subscribed and sworn to before me

this 20 day of June, 2017

Notary Public

MARY ELLEN ANGRESS
NOTARY PUBLIC OF NEW JERSEY
My Commission Expires Aug. 15, 2020