rrc risk&regulatory CONSULTING

Written By: Alan Gutierrez-Arana

Published In: The Regulator, Spring 2013

PUBLISHED ARTICLES

IT Examination Procedures in Market Conduct Exams: Taking a Deeper Look

by Alan Gutierrez-Arana, CISA, CRISC

While many industries adopted the use of computing resources with the dissemination of the personal computer in the 80s, the automation of insurance processes dates from the late 70s. Insurance companies were early adopters of automation tools for policies, claims and premiums processing and also pioneers in the development of in-house dedicated application software. Today, almost every single insurance company utilizes some type of software to compile processes and store financial and customers' information, bringing high levels of complexity to the way transactions flow and data is aggregated and processed.

The scenario described above, presents not one, but multiple challenges to the market conduct examiners. Departing from a simple question (is data accurate?), examiners have to consider three basic steps in data management: **input**, **processing** and **output**.

Input, Processing and Output

Data input processes can be as simple as an operator typing information provided by a customer in a policy form, to specialized OCR (optical character recognition) software that scans the fields in a policy form and transforms the information into digital data.

Processing includes formatting the information gathered through the input process into data that can be read by the software applications. In the case of insurance data processing, calculations are part of the data processing step; algorithms-based rates and other types of calculations are applied to the data initially received during the input step.

Output includes the generation of reports, views and printable data; this is the final product in the form of "soft" (screen visualization) copies or "hard" (printed) copies.

Data Integrity and Related Controls

Data integrity is based in the principles of consistency and accuracy. When calculations are applied to data, integrity must be ensured, even when data is transformed by those calculations. How can examiners gain assurance that data has maintained its integrity throughout the input, processing and output cycle? This is where controls come into play. In the case of automated processing, information technology controls (IT controls) play a critical role in maintaining data integrity. IT controls are a collection of measures executed by people or systems with the purpose of guaranteeing that data maintains its integrity through the entire process. IT controls are commonly group in two major categories: **IT general computer controls** and **IT application controls.**

IT General Computer Controls

By definition, information technology computer controls are activities performed inside the IT environment with the purpose of guaranteeing data and processes integrity. IT general computer controls are commonly divided into the following domains:

- Logical security: these are controls associated with the management of access to the systems and information stored and processed by those systems
- Change Management: the controls associated with the modification, update and decommission of systems, software and hardware that is part of the IT infrastructure supporting the business processes
- Systems Development Life Cycle (SDLC): all application software that is supported or created (coded) by a company must be subject to a formal SDLC in order to guarantee that it is possible to trace the translation of business requirements into algorithms and routines. These will compose the different modules of the application software utilized to automate business processes like financial management, policy management, premiums processing, and claims processing.

IT Application Controls

IT application controls are a "deeper" layer of controls in the IT environment. These controls are implemented around the input, processing and output processes executed by the systems supporting a company's business function.

Application controls can be manual controls executed by operators and related staff or automatic controls executed by routines coded in the application software. Examples of these controls are batch job execution checklists (manual) and alert flags and messages displayed by the application software to indicate any abnormality in the processing of data or instructions (automated).

Why are these controls necessary?

Without effective IT general computer controls, reliance cannot be placed in the integrity of the data stored or processed by the company's IT systems.

Overview of IT Related Examination Procedures in the NAIC Market Regulation Handbook

The NAIC Market Regulation Handbook, in its general examination standards related to operations and management described in chapter 16, considers computer systems as part of the market conduct examination procedures. The Market Regulation handbook states:

*"The examiners should determine the types of controls, safeguards and procedures for protecting the **integrity** of the computer information. The focus in this case is on those records subject to a market conduct examination that are maintained in electronic format, such as, **but not limited to**, underwriting files, claims files, rate and form filings, complaint files, statistical data used to support rates, etc." (pg. 207)*

Furthermore, Standard 2 of Chapter 16 of the NAIC Market Regulation handbook clearly refers to review of the IT computer controls in place at the examined company:

"The regulated entity has appropriate controls, safeguards and procedures for protecting the integrity of computer information" (pg. 211).

According to the handbook guidance, as part of the market conduct examination procedures, the examiner should *"ensure there is adequate security of applicant/ insured data during the electronic transference of data. Identify any areas where the applicants/insured's privacy is not properly protected" (pg.211).*

The IT related standards documented in Chapter 16 of the handbook are also applicable to examination procedures for Property & Casualty, Title Insurance, Life & Annuity, Health, and other types of insurance operations listed in the handbook.

NAIC Market Regulation Handbook Appendix F: an overlooked tool in the assessment of IT controls?

In more than one exam in which the author of this article has been involved as the IT specialist, the use and even the existence of the market regulation handbook Appendix F has been part of the discussions within the examination team. One of the reasons why Appendix F is somewhat unknown is due to the fact that the handbook does not include Appendix F. It is made available for download via the State Net website. However, Appendix F is referenced in several chapters as the tool for understanding the IT control environment in the company under examination. Appendix F covers the following IT areas:

A. MANAGEMENT AND ORGANIZATIONAL CONTROLS
B. LOGICAL AND PHYSICAL SECURITY (Systems/Environment and applications access)
C. APPLICATION MANAGEMENT
D. DISASTER RECOVERY/CONTINGENCY PLANNING
E. OPERATIONS AND PROCESSING CONTROLS

The areas listed and described in Appendix F provide a significant coverage of the control areas that examiners should expect to find in the IT environment of an insurance company. Examiners conducting market conduct exams should consider using Appendix F as part of the examination procedures, independently of the size of the company. This is a tool that has proven to be a useful resource in understanding how the companies deal with the inherent risks associated with IT environments.

Application Software Assessment Techniques in Market Conduct Exams: going the extra mile.

When conducting the field work in exams when I receive printouts like claims reports, filings, policy counts, etc. I always ask myself: How do I know that this data output I am looking at is accurate? What are the checks and balances that the system executed to guarantee that the information I am looking at is the real picture?

These questions tend to open a Pandora's Box. While IT general computer controls and application controls address many of the possible inherent risks an examiner may find during an exam, there is a deeper layer that is not normally covered: programming routines. If a company uses commercial application software (also known as Off-the-Shelf for obvious reasons) to automate its business processes, the common rule is that changes to the source code done by the company's internal development team are not allowed unless specific clauses are detailed in the contract with the vendor of the application software.

But the reality of insurance companies is quite different from other markets. Since the late 70s and early 80s, insurers typically internally developed their own application software and systems to process claims, premiums and policies. Many of those systems are still part of the core applications and systems in use at medium and large insurance companies. The in-house development of application software continues a solid trend in the insurance industry. While the initial applications were developed to run in mainframe environments using languages like COBOL, FORTRAM and other

continued on next page

older generation development languages, companies continue to develop their own applications using next generation languages for other types of computing environments like Microsoft Windows.

Following the Bread Crumb Path

How to determine if you should go down the path of reviewing programming routines? If a company has established solid systems development life cycle (SDLC) and change management controls, documentation and historic trails of coding and changes to code should be available. Examiners should look for information related to proposed changes to the application or system routine(s), impact analysis, authorization, and results of the implementation of the code or the code change into the production environment. If this information has been documented following a mature change management process, understanding the nature of the routines that process insurance related data should be an easy task and identification of control points will be transparent to the examiner. Some of the characteristics of programming under a mature SDLC and change management control environment are:

- Version control process is in place
- Change management log is embedded in the precompiled code with programmer's signature
- Code is properly indented
- Modified code is commented and not deleted
- Naming conventions are utilized in accordance with guidelines
- Modular Top-Down flow is utilized

If you find the characteristics listed above as part of a system or application software documentation, the level of confidence on the control environment could be considered high and the output data produced by the systems supporting the business processes can be considered reliable.

The Black Box Scenario

In the event that the insurer has not established mature processes for SDLC and change management, the examiner is faced with a significant challenge: what are the routines and algorithms inside the system? How do I determine whether the actual data output produced by the system is accurate?

When applications are incorrectly coded or controls are not implemented around changes to the algorithms and other elements of the code, the probability that the data output produced by the system is inaccurate is relatively high. Some of the signals that examiners should look for are the amount of manual corrections done by the insurer to its policies, premiums and claims data. If the number of corrections is high, it is clear that application controls are not effectively addressing the risks associated with automated processing and the examiner should determine if the data produced by the systems can be considered reliable or if detailed testing is required. If the assistance of IT specialists with programming knowledge is available, the examiner should consider the review of the application code considering the following programming best practices:

- Precision, clarity, lack of ambiguity
- Consistency
- Relevancy
- Testability
- Traceability

If the characteristics above are found during a code review exercise, the application output can be considered reliable.

In a Nutshell

The chances of finding automated systems processing policies, premiums and claims in an insurance company are almost a certainty for the examiners conducting market conduct examination procedures. While the majority of companies have implemented SDLC and change management process controls around these processes and control maturity has been achieved, there will always be where those controls are not implemented or are not operating in an effective manner. The utilization of Appendix F of the NAIC Market Regulation handbook is a good first step to understand the control environment around the automated processes utilized by the insurer to process data related to policies, claims and premiums.

If the examiner is faced with an environment in which controls have not been implemented or are not in a mature stage, conducting a more in-depth analysis of the application code combined with detailed testing of the data during the input, processing and output should be considered as part of the examination process. ■

Alan Gutierrez-Arana, a director with Risk & Regulatory Consulting, has over 15 years of experience providing IT security and controls assessments, and regulatory compliance consulting services for a broad range of insurance, banking, finance and high technology entities. He specializes in IT controls assessment and compliance, federal and state IT regulatory compliance (NAIC, SOX, PCI-DSS, HIPAA-HITECH, BASEL II, FFEIC), controls design and implementation, disaster recovery, IT outsourcing and off-shoring, IT governance, business continuity, change management, information security, and e-business; his client portfolio includes several insurance departments, Fortune 100 and Fortune 500 companies."