Description of Gallagher Bassett Services, Inc.'s RISX-FACS® System and Claims Processing for U.S. and Canadian Operations Throughout the Period 1 November 2012 to 31 October 2013

With the Independent Service Auditor's Assurance Report,
including Tests Performed and Results Thereof

Service Organization Control 1 Report

Gallagher Bassett Services, Inc.

Gallagher Bassett Services, Inc.'s RISX-FACS® System and Claims Processing for U.S. and Canadian Operations

Gallagher Bassett Services, Inc.’s Management Assertion

Gallagher Bassett Services, Inc.

Gallagher Bassett Services, Inc.'s Management Assertion

13 December 2013

We have prepared the accompanying Description of Gallagher Basset Services, Inc.'s RISX-FACS® System and Claims Processing for U.S. and Canadian Operations (Description) for users of the system during some or all of the period 1 November 2012 to 31 October 2013 (user entities), and their independent auditors who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. The management of Gallagher Bassett Services, Inc. confirms, to the best of its knowledge and belief, that:

a. the Description fairly presents the RISX-FACS® System and Claims Processing for U.S. and Canadian Operations (System) made available to user entities during the period 1 November 2012 to 31 October 2013, for processing their transactions. The Service Organization uses the following subservice organizations: (1) Citibank N.A. for U.S. bank accounts for certain cash management and payment controls and (2) Medrisk, Corvel, Genex, Bunch and Coventry for review and repricing of submitted claims meeting certain criteria. The Description includes only the controls and related control objectives of the Service Organization and excludes the control objectives and related controls of Citibank N.A., Medrisk, Corvel, Genex, Bunch and Coventry. The criteria we used in making this assertion were that the Description:

   (1) presents how the System made available to user entities was designed and implemented to process relevant transactions, including:

   - the types of services provided, including the classes of transactions processed.
   - the procedures, within both automated and manual systems, by which those services are provided, including by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities.
   - the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities.
   - how the System captures and addresses significant events and conditions, other than transactions.
   - the process used to prepare reports or other information provided to user entities.
   - specified control objectives and controls designed to achieve those objectives.
   - controls that, in designing the System, we contemplated would be implemented by user entities in order to achieve the specified control objectives (Complementary User Entity Controls).

- other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to the services provided, including processing and reporting transactions of user entities.

(2) does not omit or distort information relevant to the scope of the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities and their independent auditors, and may not, therefore, include every aspect of the System that each individual user entity and its independent auditor may consider important in the user entity's own particular environment.

b. the Description includes relevant details of changes to the System during the period from 1 November 2012 to 31 October 2013.

c. the controls related to the control objectives stated in the Description, which, together with the complementary user entity controls and subservice organization's controls referred to above if suitably designed and operating effectively, were suitably designed and operated effectively throughout the period 1 November 2012 to 31 October 2013, to achieve those control objectives. The criteria we used in making this assertion were that:

(1) the risks that threaten the achievement of the control objectives stated in the Description have been identified by the service organization;

(2) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

(3) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely,

Management of Gallagher Bassett Services, Inc.

Independent Service Auditor’s Assurance Report

Ernst & Young LLP
155 North Wacker Drive
Chicago, IL 60606-1787

Tel: +1 312 879 2000
Fax: +1 312 879 4000
ey.com

The Executive Committee
Gallagher Bassett Services, Inc.

Scope

We have examined Gallagher Bassett Services, Inc.'s accompanying Description of its RISX-FACS® System and Claims Processing for U.S. and Canadian Operations throughout the period 1 November 2012 to 31 October 2013 (Description) and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of Gallagher Bassett Services, Inc.'s controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Gallagher Bassett Services, Inc. uses the following subservice organizations: (1) Citibank N.A. for U.S. bank accounts for certain cash management and payment controls and (2) Medrisk, Corvel, Genex, Bunch, and Coventry for review and repricing of submitted claims meeting certain criteria. The Description includes only the controls and related control objectives of Gallagher Bassett Services, Inc. and excludes the control objectives and related controls of Citibank N.A., Medrisk, Corvel, Genex, Bunch, and Coventry. Our examination did not extend to controls of Citibank N.A., Medrisk, Corvel, Genex, Bunch, and Coventry.

The information in the accompanying "Other Information Provided by Gallagher Bassett Services, Inc." is presented by management of Gallagher Bassett Services, Inc. to provide additional information and is not part of Gallagher Bassett Services, Inc.'s Description. Such information has not been subjected to the procedures applied in our examination, and accordingly, we express no opinion on it.

Gallagher Bassett Services, Inc.'s responsibilities

Gallagher Bassett Services, Inc. has provided the accompanying assertion titled "Gallagher Bassett Services, Inc.'s Management Assertion" (Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description. Gallagher Bassett Services, Inc. is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls to achieve the related control objectives stated in the Description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Our examination was also performed in accordance with International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we comply with ethical requirements and plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls described therein are suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period 1 November 2012 to 31 October 2013.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls described therein to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives, and the suitability of the criteria specified by the service organization and described in the Assertion. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their independent auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions or identification of the function performed by the system. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in Gallagher Bassett Services, Inc.'s Assertion:

a. the Description fairly presents the RISX-FACS® System and Claims Processing for U.S. and Canadian Operations that was designed and implemented throughout the period 1 November 2012 to 31 October 2013.

b. the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 1 November 2012 to 31 October 2013, and if user entities applied the complementary user entity controls contemplated in the design of Gallagher Bassett Services, Inc.'s controls, and if

subservice organizations applied the controls contemplated in the design of Gallagher Bassett Services, Inc.'s controls throughout the period 1 November 2012 to 31 October 2013.

c. the controls tested, which, together with the complementary user entity controls and subservice organizations' controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period 1 November 2012 to 31 October 2013.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying "Description of Control Objectives, Controls, Tests, and Results of Tests" (Description of Tests and Results).

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Gallagher Bassett Services, Inc., user entities of Gallagher Bassett Services, Inc.'s RISX-FACS® System and Claims Processing for U.S. and Canadian Operations during some or all of the period 1 November 2012 to 31 October 2013, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

13 December 2013

Description of Gallagher Bassett Services, Inc.'s RISX-FACS® System and Claims Processing for U.S. and Canadian Operations throughout the period 1 November 2012 to 31 October 2013

General Information

Gallagher Bassett Services, Inc. Profile

Gallagher Bassett Services, Inc. (Gallagher Bassett, the Company or GB) is a wholly owned subsidiary of Arthur J. Gallagher & Co. (AJG), an insurance brokerage company founded in 1927 as an insurance agency. Gallagher Bassett offers services on either a totally integrated or stand-alone basis through the following four core businesses:

- **Claims Management** — Provides claims management services mainly through the Field Operations division, which has a nationwide network of branch offices that are grouped by zones and areas.
- **Gallagher Bassett Information Technology (GBIT)** — Provides claims management information services to clients and the Gallagher Bassett and AJG user communities.
- **Risk Control Consulting Services** — Provides risk control consulting services, which focus on clients' needs to control losses and loss exposures.
- **Appraisal Services** — Determines replacement valuation costs of buildings and contents to help ensure adequate protection against financial loss.

Claims management services are offered through the Claims Management and GBIT divisions.

Claims are processed primarily using Gallagher Bassett's RISX-FACS® Classic system. The RISX-FACS® Classic system runs on a Hewlett-Packard (HP) NonStop computer and was originally developed in-house in the early 1980s. RISX-FACS.com® was introduced in 2000 and provides users with the ability to browse their accounts for the status of their claims and to submit basic pieces of information for processing. In 2010, Gallagher Bassett introduced RISX-FACS.net® loss setup/maintenance and claim setup processing. RISX-FACS® is used by Gallagher Bassett clients, Gallagher Bassett, and AJG users. RISX-FACS.com® and RISX-FACS.net® services are both available to the same user population. Going forward within the report, the aforementioned systems will be collectively referred to as RISX-FACS®.

MYGBCLAIM.com® provides claimants with read-only online access to their check and payment status information. After claimants have been appropriately authenticated, they have access only to information related to their respective claim(s).

Gallagher Bassett has a diverse client base, including industrial and commercial operations, municipalities, religious and educational institutions, and health care organizations. Gallagher Bassett's corporate headquarters is located in Itasca, Illinois.

Description of Operations

Gallagher Bassett is organized into distinct profit and expense centers. Each profit center delivers its products and services on a decentralized basis through various branches located within the U.S. and Canada. Expense centers, most of which are located in the corporate headquarters in Itasca, Illinois, serve all divisions of Gallagher Bassett.

There are three organizations vital to Gallagher Bassett's claims processing:

- Claims Management
- GBIT
- Finance

Each of the above profit and expense centers report to the President of Gallagher Bassett, who, in turn, reports to the President and CEO of AJG.

Claims Management

Claims Management is Gallagher Bassett's largest profit center. The Field Operations division delivers claims management services to clients through a nationwide network of branch offices, which are grouped by zones and areas. The network is centrally managed, and all branches are required to follow the servicing standards established by Claims Management. Additional services are provided through National Account Management, which assigns an Account Manager to large accounts to serve as a liaison between the client and Gallagher Bassett.

GBIT is dedicated to delivering management information services to clients and the user communities of Gallagher Bassett and AJG. GBIT has primary responsibility for:

- **RISX-FACS® Classic** — Risk Financial and Administrative Control System, which runs on an HP NonStop computer and provides processing for claim and loss information.
- **RISX-FACS.net®** — Risk Financial and Administrative Control System, which utilizes a .net design. Access today is primarily for internal Gallagher Bassett personnel. It provides certain converted classic processing functions for claim and loss information.
- **RISX-FACS.com®** — Risk Financial and Administrative Control System accessed by Gallagher Bassett clients, Gallagher Bassett, and AJG users through the internet. The client signs on at the internet site and is authenticated to the RISX-FACS® system. The software permits online access for clients to view various claims and losses for their respective client ID.
- **RISX-FACS® Reporting** — The Standard Report Package is a collection of monthly, quarterly, and annual summary and analysis reports prepared for claims management clients. Print and download options are available. SELEX-FACS®, Analysis Workbench (AWB), and I-Link are online software tools that permit users to create ad hoc reports for download.

GBIT consists of the following functional groups:

- **Product Management** — Product Strategy, Competitive Analysis, User Management.
- **Architecture**
- **IT Portfolio Management**
- **ADM** — Applications Development & Maintenance, Technical Design & Analysis, Change Management, Business Analysis.
- **Business Office** — Metrics and Management Reporting, Financial Management, Program Office, Compliance, Asset Management.
- **Technical Operations** — Vendor Management, Information Security, Business Continuity/Disaster Recovery, Production Support, Database Support, New Client Implementation, and Management of Gallagher Technology Services (GTS) — shared services provided by GB's parent AJG, which include support of the aforementioned technical operations, network and telecom capabilities, operations support desk, remote access capabilities, and messaging (email, calendar).

Finance

Finance is an expense center responsible for various centralized Gallagher Bassett functions, including client banking functions, which are performed by the Client Financial Services (CFS) Department. This department consists of two areas: the banking unit and the recovery unit. The banking unit is primarily responsible for the day-to-day maintenance of all client banking relationships. Major responsibilities include account reconciliation, stop-payment processing, and bank charge monitoring. The recovery unit is responsible for the processing of all claim recoveries except excess recoveries, which are handled by the Gallagher Bassett Quality Department.

Significant accounts or classes of transactions

Accounts that may be affected by transactions processed through RISX-FACS® may include cash, claims, liabilities, expenses, and reserves.

Third-Party Outsourcing Arrangements

Sub-Service Organizations

Gallagher Bassett utilizes the following subservice organizations to provide banking and certain claims review and repricing functions. The controls in scope for this report include only those policies, procedures, and control objectives at Gallagher Bassett and do not include policies, procedures, and control objectives at the subservice organizations.

- Citibank N.A. — (for U.S. Citibank bank accounts) supports the APACS/SIMMS claim payment processing function for Gallagher Bassett. Individual demand deposit accounts are established for purposes of depositing client funds and making claim payments per established Claims Management procedures. Check issuance data is transmitted to Citibank N.A. each day to establish the Positive Payment framework with enhanced Payee, Name, and Authentication (PNA) as part of the antifraud detection process. Citibank N.A. has a Canadian branch that contains GB client bank accounts; however, the Citibank functions mentioned above are not being utilized for cash management or payment controls of the Canadian Citibank bank accounts.

- Several third-party managed care service providers are used for review and repricing of submitted medical bills meeting certain criteria. Medrisk, Corvel, Genex, Bunch, and Coventry are the main providers. Gallagher Bassett sends the claim information to the repricing service organization for review of the charges. The managed care service organization reviews the claim information provided against defined criteria and determines action to take on the charges, including actual charges to consider.

Service Vendors

Gallagher Bassett utilizes the following service vendors to perform certain functions to improve operating and administrative effectiveness. The services provided by these vendors are included in the description of Gallagher Bassett's processes and controls below; however, they do not affect the controls or control objectives.

- Data center services are outsourced to a separate hosting facility. In early November 2012, data center services were moved from Verizon Business Services to SAVVIS Services, the hosting service organization that is responsible for the physical security of the facility and the underlying infrastructure availability of the external environment. Development and Quality Assurance (QA**)** systems remain on-site in Gallagher Bassett's Itasca data center.

- Medical bill imaging service organizations, primarily Coventry and Jopari, are used for imaging the majority of medical bills and charges from medical providers received by Gallagher Bassett. Medical bills from Gallagher Bassett clients and claimants are received by the medical bill imaging service organization, scanned, examined, and loaded into Gallagher Bassett's RISX-FACS® application. Medical bill imaging service organization personnel have the ability to query RISX-FACS® for claimant and group information throughout the medical bill imaging and error correction processes.

- Check-printing service organizations, MicroDynamics Group and Citibank N.A. (through Moore), are used for printing and mailing of claim payments and correspondence originating from the RISX-FACS® application. The check-printing service organization receives nightly files from Gallagher Bassett of activity processed for the day. These files are loaded and processed, resulting in the printing and mailing of claims payments and correspondence.

- Preliminary reviews for coverage issues are partially performed by Crossdomain Solutions on some accounts. Crossdomain personnel (along with other Gallagher Bassett team members) review certain newly reported losses received by Gallagher Bassett, update a coverage "010" note per Gallagher Bassett best practices and any client-specific instructions/requirements and attach appropriate coverage documentation to the file.

Company-Level Elements

Control Environment and Organizational Structure

A management committee consisting of Gallagher Bassett's executive management oversees Gallagher Bassett's operations and determines the strategic direction of the Company. Counsel embedded in Gallagher Bassett or AJG's legal counsel will assist Gallagher Bassett in matters requiring legal assistance. The executive committee of Gallagher Bassett management meets on a monthly basis to discuss activities at Gallagher Bassett.

Gallagher Bassett management prepares and distributes a three-year strategic plan. Departmental activities are designed to meet these strategies and goals. The roles and responsibilities within the various departments are documented, reviewed and updated regularly. In addition, a code of business conduct and ethics is signed by employees to demonstrate their intent to comply.

Gallagher Bassett has formal hiring practices that are designed to help ensure new employees are qualified for their job responsibilities. All personnel are subject to background checks.

New Gallagher Bassett claims processors attend an in-house training program and undergo supervision once training has been completed. On-the-job training, periodic meetings with departmental personnel, and written communications serve as additional training for Gallagher Bassett employees. All new employees are required to view the antifraud video produced specifically for Gallagher Bassett. The VP of Risk Management periodically conducts fraud training and sends out written communications on fraud topics as needed. Conflict-of-interest statements are signed by all Claims Management employees on an annual basis. The VP of Risk Management coordinates this effort together with the Corporate Legal staff.

Formal written performance reviews are conducted on an annual basis. Employees are evaluated on objective criteria.

Risk Assessment Process and Control Activities

Policies and procedures have been established to help ensure that claims payments are consistent with the client service agreements, that inappropriate action by a claims processing staff member is prevented, and that proper financial controls and appropriate separation of work procedures are in place to handle those client dollars accordingly.

Designated personnel monitor the IT environment to prevent and detect any inappropriate activity originating from outside the network and fraudulent activity within the network.

Management performs a company-wide IT risk assessment at least every two years, which translates to specific mitigation activities and remediation efforts. This process is one of many key controls that are in place to address the Company's Sarbanes-Oxley governance, and the responsibility is owned by the Corporate Chief Information Officer. The risk assessment is done in conjunction with the Company's Internal Audit lead and a third-party organization that specializes in this area. A formal risk assessment associated with Gallagher Bassett's claims processing operations is completed twice a year.

Information and Communication

Gallagher Bassett's management is committed to maintaining an environment of open communication with all employees. Updates on the Company's performance and other relevant matters of interest are communicated through a number of outlets, including internal newsletters, quarterly press releases, the Company's intranet, email distribution, meetings with managers, and Gallagher Bassett's written policies/procedures for which the Company routinely provides ongoing training.

Gallagher Bassett's policies are documented and accessible via the Company's intranet. Documented policies relate to financial management; operations; information technology; human resources; service delivery; claims best practices; and benefit administration, audit, and compliance. These Company policies provide a formal standard and serve as a foundation for the development of more detailed procedures.

A fraud hotline is available 24 hours a day for Gallagher Bassett employees to report possible cases of internal fraud.

Monitoring

Process and control management at Gallagher Bassett operates through the defined management structure. System-generated information is used by management to assist them in monitoring processes and controls. In addition, there is an array of internal and external audits that are performed.

Monitoring controls begin within Claims Management. The Branch Manager or the Operations Supervisor (where one exists) is responsible for monitoring claim activity in their respective office. The Branch Manager, Area Vice President, Senior Vice President, and, ultimately, the EVP of U.S. Claims Operations are all responsible for monitoring specific pieces of the claims administration activity and taking action as necessary.

Compliance management at the branch level is evaluated via direct review of claim file activity. Supervisors are required to periodically (within 100 days for most files) review files for compliance to Gallagher Bassett's internal product standards and Client Service Instructions (CSI). Other parties in the compliance chain review a subset of the overall claims activity.

The VP of Risk Management uses a program related to internal and external fraud prevention and detection to actively monitor various aspects of Gallagher Bassett's operations for possible instances of fraud. Advanced data analytics and various system-generated reports are used as part of the monitoring process. The Gallagher Bassett Quality Department, independent of field operations, is responsible for auditing branch activity. The role of the Quality Department is to facilitate and validate audit sample selection, as well as conduct monthly Quality Assurance (QA) audits on a percentage of Service Center audits. Each branch is audited monthly, with the results reported to field operations management. There are monthly, quarterly, and year-to-date audit scores for each adjuster. Approximately 4,500 files are audited each month.

Description of Controls

Data and Procedural Controls

Overview

RISX-FACS® is an online transactional system that does not require batching for normal claims and payment processing. Tens of thousands of other jobs are handled each day through differing scheduling methods. Examples of critical and time-sensitive processes include, but are not limited to, Banking, Loss Maintenance, Data Transfers, Monthly Reports, Electronic State Reporting (ESR), and Nurse Notes. Netbatch, a native HP NonStop system application, is used for regular, predictable, and repetitive batch jobs. Ad Hoc is used for on-demand batch processing where no manual processing or intervention is required, but system resource balancing may be required.

Manual and non-routine requests are handled by GTS when none of the automated scheduling mechanisms are appropriate.

Netbatch Scheduler

Netbatch jobs are completed by a scheduling system. Access to the Netbatch scheduling system is limited to personnel in the Operations and Production Support Departments (Control 1.01). Normally, only jobs that have been requested to be completed on a desired frequency are included in this scheduling system. Requests come into the Schedulers via email. The Schedulers review the request to help ensure user role validity (based on departmental responsibilities and roles) and logistical viability (based on available resources, file, job contentions, etc.). If the schedule request is appropriate, the Schedulers input the job into Netbatch (Control 1.02).

If a failure occurs with the running of a Netbatch job, a warning appears on the UTT94 error consoles (Control 1.03). CHECKSYS, a GBIT-created Tandem Advanced Command Language (TACL) routine, is used to monitor critical system applications and sends automated alerts for scheduled job errors/failures. In addition, major processes, such as the LMQ90 Daily Electronic Data Interchange (EDI) Transmission from Vendors, send internal email notifications per success or failure, as well as log events into the System Error Log. Every major/critical process has associated written procedures developed to include unique notification/escalation and handling steps. These instructions may include handling of errors or escalation criteria, along with service-level agreements (SLAs).The operations lead or manager may also participate in the escalation process when procedures are in question. Processes are handled or escalated per predefined written procedures and documented in the Daily Activity Summary. Any outstanding process is communicated for shift turnover for continued monitoring and follow-up (Control 1.07). Only failures related to major/critical jobs that can be resolved by operations staff are documented to resolution in the Daily Activity Summary (Control 1.04). When operations staff cannot resolve a failure, escalation procedures are followed to gain involvement of additional resources that can assist with addressing the failure.

Ad Hoc Scheduler

A screen within RISX-FACS® allows users to request Ad-Hoc jobs for certain reports. Examples of these jobs include, but are not limited to, SELEX-FACS® reports, Build-A-Record®, and other user-scheduled reports. These reports are not used by GB for processing claims and are delivered to end users and clients for informational purposes only. The request to run Ad-Hoc jobs is submitted online and is completed by an Ad-Hoc scheduling system. This system runs the reports through batch primarily on a first-in, first-out basis but also balances performance conditions and job dependencies. Jobs are scheduled in advance and are automatically submitted to the Ad Hoc Scheduler. Jobs that are owned by other user IDs can be modified only by appropriate individuals within Operations and Client Support Services. The ability to submit an Ad Hoc job is limited through RISX-FACS® Security to the SELEX-FACS® online screen (Control 1.01). Users may cancel their own scheduled job, but may require Operations intervention if the job has already started. Functions and features in the Ad Hoc Scheduler are managed through the System Development Life Cycle (SDLC) process.

If a failure were to occur with the running of an Ad Hoc job, a warning would appear on the UTT94 error consoles. Errors are monitored and escalated to appropriate departments accordingly. For example, database errors are routed to Database, programmatic errors to Application Development, or conditions when the file is full to the Operations Lead. If immediate resolution of the error is necessary, it is the responsibility of the functional area or department to which the issue is escalated. If immediate resolution is not required, resolution is scheduled by the functional area or department as appropriate. If a problem originated from the Help Desk, a Remedy ticket would remain open and require follow-up with the escalation team to work the ticket to closure. Problems reported outside of the Remedy ticket system are logged, recorded, or escalated as appropriate.

Manual Jobs

Manual jobs include daily activities and non-routine job requests. Access to the manual job execution is limited to personnel in the Operations and Production Support Departments (Control 1.01).

Daily activities are the regularly planned, scripted, manually entered, or triggered tasks that are performed by the operators every day in the course of normal job processing. As activities are completed, the operator running the job signs off on the schedule and indicates the time of completion. The Daily Activity Summary is used as a guide for scheduling and completing jobs for the day (Control 1.05).

Non-routine job requests are as-needed job requests that are submitted throughout the course of business directly to the Scheduling Department. Non-routine job requests must be written on hard copy or email form; no verbal requests are accepted (Control 1.06). Requests can come from the GBIT Application Development & Maintenance team, CFS, the GBIT Data Run-In team, or the GBIT Database team, for example. Only requests appropriate and pertinent to the requesting department are approved by management. The Operations Manager and Operations Lead monitor requests and may offer consultation as deemed necessary. Requestors forward a form located on the intranet or an email to the Schedulers' shared email box. The Schedulers are responsible for scheduling jobs based on the submitted requests. The Scheduler determines that the request has all information required to run the request. Unless approved by a manager for "emergency" status, non-routine requests are deferred to nonbusiness hours (i.e., 7:00 p.m.–7:00 a.m.) to avoid a potentially negative impact on the system. An email is sent to the requestor verifying receipt of the request, and another email is sent when the request is completed. A status is supplied to the requestor every 24 hours until the request is completed or canceled by the requestor. These jobs may include special one-off programs such as a unique data transfer, special report, Data Run-In, or special external data loads.

If a failure occurs with daily activities or non-routine requests, a warning appears on the UTT94 error consoles and/or the individual console running the program. Any issues encountered when processing a request are forwarded back to the requestor for resolution and follow-up. It is the responsibility of the requestor to address the problem and determine if the job must be resubmitted.

Other Information

GB Operations has three turnover meetings per day to discuss the status of the daily activities, non-routine job requests, and issues encountered. The Daily Activity checklists, non-routine job requests, and the turnover form are reviewed and explained at the start of each shift (Control 1.07). Any further clarification or special instructions are communicated during these meetings. The turnover form is used to track non-routine job requests not completed during the prior shift. There are designated GB Operations management personnel to contact in case problems require management intervention. These personnel are identified in the Disaster Recovery Manual (Controls 1.08 and 3.05).

Access to Data Files and Programs

Internal user logical access to the RISX-FACS® application and its underlying infrastructure (HP NonStop) is administered by the GB Security Administration group at the corporate home office. RISX-FACS® access is provisioned based on the job role and associated security job template (Control 2.03). Access request forms are located within the web-based Gallagher Bassett Security System. A request for access to RISX-FACS and/or HP NonStop comes from a manager or authorized representative and is submitted via the Gallagher Bassett Security System. The submission/request is automatically processed based on the type of job role selected. Internal users are assigned a job template, which defines the standard authorizations for the job role. Exceptions to job templates require manual steps by the Security Administrator (Control 2.02). Access will be granted as of the effective date indicated on the security web request unless additional approvals are required. If approvals are required, email notifications are sent to the approvers, who click on a link in the email to make the approval or rejection. After all approvals are made, the request will be processed. The submission creates a system-generated email that is sent to the GB-Security email account for review, approval, and, in certain cases, additional manual processing. After the request is reviewed by the Security Administrator, it is set up as requested. Request forms are retained in emails and an SQL database.

The same process is followed when modifications to existing IDs are required.

Client user logical access is offered to Gallagher Bassett clients, carriers, brokers, auditors, managed care users, vendors, and AJG users. This access is only limited update and read-only mode, or grants the user the ability to add claim notes (Control 2.04). Client user access is authorized and administered by Gallagher Bassett Account Executives, Account Managers, and/or their Technical Support staff. Client requests requiring additional approval, such as requests for reading California claim medical notes or requests from managed care users and carrier users, are routed to the Security Administrator or Designated Approver for further authorization and approval processing.

A procedural manual located on the Company's intranet exists for users of the Security Request System for administering user access, such as additions of new users, changes to existing user accounts, deletion of terminated users, and "thawing" a user's account. Thawing refers to the reactivation of an account after it has been disabled (Control 2.01).

Application Access

RISX-FACS® is used by Gallagher Bassett employees to view/process loss and claim-related transactions. A RISX-FACS® user ID number is required to access the RISX-FACS® system.

For new employees, a request can be submitted up to two weeks in advance of the start date. Password settings for RISX-FACS® are set to enforce expiration, length, lockout, history and complexity (Control 2.07). For claims processing branches, the Security Administrator follows several steps when assigning the employee to the appropriate clients:

- For a branch user, a default client list is assigned based on the authorized clients for the branch. The requestor can modify the default client list as necessary for that user.
- If the user is someone other than a branch user, the security request form identifies the clients that the user is granted access to.
- If it is a new client, the Account Manager supplies the information and the payment authorization to be established for the client.

There are two ways to access the RISX-FACS® applications:

- Client users must enter their unique user ID and password into the secured website.
- Internal Gallagher Bassett and AJG users must first log on to the network services and then enter their RISX-FACS® user ID and password.

RISX-FACS® Security reads the rules database (a repository for access levels per user), reviews the user's account, and determines the access levels authorized (known as a damage factor) when a user initially accesses the system. Users will only be shown a menu that correlates with the access level within the system.

Claims adjusters are automatically given the authority to issue checks and enter claim notes. Clerical personnel are given the authority to check the items designated on the security request form. Clerical personnel may be set up with or without check issuance authority.

e-Invoice/e-Bill Access

Security to the e-Boxes (electronic mail boxes set up for each adjuster) is set up so that adjusters have the authority to share e-Boxes (an adjuster from one branch cannot access the e-Box of an adjuster from another branch). Adjusters each have the authority to share their e-Box, and all adjusters within the same branch and with the same client access have the authority to share adjuster e-Boxes (Control 2.10); therefore, if one adjuster is on vacation, another adjuster (with the same client authority) can manage the e-Box of the adjuster on vacation. When e-bills/e-invoices are paid or rejected, the adjuster ID of the owner of the e-Box and of the adjuster approving or rejecting the payment is recorded in RISX-FACS®. Although an adjuster has the capability to access another adjuster's mailbox,

access must be done through the adjuster using his or her designated ID. The Canadian branch processes bills that are paper-based; no e-Box is available for claims processing.

Termination of Access

For internal users, termination of security is requested by the branch manager or authorized representative using the automated Gallagher Bassett Security System. The requestor submits an electronic termination notice within the Security System, specifying the requested date and time of access termination. Upon submission, the electronic notice triggers the Security System to automatically terminate the user's ID on the date and time requested using an HP NonStop command. The user's RISX-FACS® client and application security access is removed, and the user ID is placed in a terminated state (Control 2.05). The Security Administrator is notified of the termination and any special comments via an electronic notification generated by the Security System. The Security Administrator initiates the disabling of the user's Active Directory account for non-GB employees. For GB employees, Active Directory is terminated by an off-boarding request. The Security Administrator removes Tandem Access Command Language (TACL) security within a reasonable time based on the date and time of the termination request. The work assigned to the employee's ID will still function normally until the work is moved to another employee. Termination of client user access is directly handled by the Account Managers or their Technical Assistants. The Security Administrator can also handle the terminations of client user access. The client contact is responsible for initiating these termination requests and ensuring accuracy. For example, if Coventry terminates a nurse/nurse's access, Coventry notifies Managed Care within Gallagher Bassett and submits a termination notice to IT to terminate access.

In addition to removing RISX-FACS® security upon termination notification, the Security Administrator is responsible for resetting a user's TACL account once locked out. RISX-FACS® and TACL are set up to freeze or suspend a user's account after a user makes four unsuccessful attempts to log on to RISX-FACS® or TACL. The AJG Shared Services Help Desk is responsible for resetting a user's RISX-FACS® account after verifying the last four digits of the user's Social Security Number (SSN). Documentation related to the freeze and thaw is retained by the AJG Shared Services Help Desk.

Periodic Review of RISX-FACS® User Access

On a quarterly basis, a system-generated listing of active internal GB users by branch is sent to the applicable branch manager for review. Included in the branch report are the branch number, branch name, employee number, employee name, authorization IDs, authorization ID descriptions, and damage factor information. Each branch manager must review the columns of the spreadsheet, confirming that the user is active and also that the user should have the authorizations assigned to him/her. The spreadsheet is to be emailed back to the Security Administrator. Termination of security is requested by the branch manager or authorized representative using the Gallagher Bassett Security System (Control 2.06). Copies of the outgoing audit spreadsheets and completed spreadsheets are stored in a Sharepoint database, as well as in hard-copy form in a file. Clients and Managed Care vendors are responsible for periodically reviewing access levels for client and managed care (i.e., nurses) personnel to determine whether the access is appropriate. Branch personnel request changes via the RISX-FACS® security website and completed under oversight of the GB Security Administration group.

HP NonStop Operating System Access Security

HP NonStop users (GBIT and certain Claims Management users) are authenticated by Safeguard security, which requires a user ID and password. Password parameters, such as password history (cannot reuse last 13 passwords), minimum length (eight characters minimum), and password complexity (must maintain both alpha and numeric or special characters) are enabled. Users are required to change their passwords every 90 days, except SUPER IDs, which are required to change passwords every 30 days (unless a valid policy exception is on file). HP NonStop security is set up to freeze accounts after 90 days of inactivity. Accounts are locked after four unsuccessful logon attempts (Control 2.07).

Access security to the HP NonStop operating system is administered in the same manner as described for RISX-FACS®, and access to privileged accounts is appropriately restricted to personnel in GBIT (Control 2.09).

HP NonStop Security Logs

GBIT has developed a $CMON process to monitor and control access to the HP NonStop operating system. This process is applicable to GBIT users and those GBIT users accessing certain SUPER IDs.

GBIT employees initially sign on to the HP NonStop system through Guardian, which enforces the security rules for HP NonStop, under their Guardian ID. Initial sign-on is logged. If a user wishes to use one of the SUPER IDs, he/she must then sign on as the appropriate SUPER ID. Before allowing access, $CMON interrupts the sign-on message and searches a security table to validate the request.

When the user is signing on, a record is written to the HP NonStop log file detailing the user that signed on, the SUPER ID that the user is accessing, and the terminal. The processes that are being affected by the SUPER ID are logged. In addition, failures to log on to the system are recorded and reviewed as part of the weekly monitoring process described below (Control 2.09).

The log can be examined online. Reports are generated on a weekly basis for super user account access, log-ons by users, and configuration and object changes. The reports are reviewed by the Director of Systems Security in GBIT (Control 2.08). Any review issue encountered is addressed as appropriate by the Director of Systems Security.

Access to Data Facilities

Production data center operations are outsourced to a separate hosting facility. In early November 2012, production data center operations moved from the Verizon Data Center to the SAVVIS Data Center. The hosting service organization is responsible for the physical security of the facility and the underlying infrastructure availability of the external environment. As Gallagher Bassett's production site is housed at a third-party location, a review is performed by the Global IT Security group (a sub group of GTS) on a quarterly basis over all users (third-party, Gallagher Bassett, and AJG staff individuals) with access to both the Verizon (through early November 2012) and the SAVVIS (beginning November 2012) Data Centers (Control 2.11). If any changes to access are required, they are submitted to Verizon/SAVVIS to make the modification.

Tape and File Management

Backup

The HP NonStop operating system is backed up to virtual tape based on file types: non-audited and audited files. Non-audited files include files such as extracts for batch jobs, file structures, file locations, and log files. These files are incrementally backed up every day throughout the week and fully backed up once a week on the weekend (Control 3.01). Files are incrementally backed up if they have changed within 24 hours based on the last update date and time noted in the system. Any failed backup job generates an on-screen error message. Operators assigned to monitor the process manually restart the job per defined procedures (Control 1.04).

Audited files include claims transaction data files such as client claims and client payments. These files encompass approximately 98% of the HP NonStop operating system's databases. When a transaction is entered into the system, the changes are written to an audit trail file via HP NonStop Transaction Monitoring Facilities (TMF) functionality. TMF takes before and after snapshots of all records related to a transaction, which are then stored in the audit trail file. As the audit trail files meet the file's storage limit, they are moved to virtual tape. The TMF audit trail is incrementally backed up every day throughout the week. In addition, a full online dump is completed once a week on the weekend. Given TMF's functionality, GBIT has the ability to restore data to any point in time in the past five weeks.

Access to modify backup and restore management jobs are restricted to personnel in the Operations group. This is controlled by HP's Safeguard security (Control 3.02).

Annually, members of GBIT perform a full disaster recovery test. The backup data center houses hardware that is equally as capable of supporting RISX-FACS® as the production hardware housed at the SAVVIS Data Center (Control 3.04).

Tape Management

Gallagher Bassett uses TMF to manage backups for audited files on the system, which includes the client database. TMF has its own tape catalog to keep track of tapes in use and scratch tapes. TMF tapes reside on the virtual tape system. Other non-audited tapes are managed by HP's Mediacom for full and partial backups. Special backups are entered into a Gallagher Bassett tape catalog, which is viewed on the virtual tape system as an externally labeled tape.

For greater reliability and decreased recovery times, Gallagher Bassett utilizes virtual tapes containing both audited and non-audited files. Virtual backup tapes are maintained on the Production system, located in Elk Grove, Illinois (beginning November 2012 — prior to November 2012, the tapes were maintained in Manassas, Virginia), as the on-site copy. These virtual tapes are also copied to the disaster recovery virtual tape system located in Itasca, Illinois, and maintained there for disaster recovery. These tapes are considered the off-site tapes (Control 3.03). The virtual tape system has an interface that allows Operations to manage the tape copies. Virtual tapes are retained in accordance with the corporate backup retention policy.

Application Development, Maintenance, and Documentation

Change Request

Gallagher Bassett has a formally documented process for the development and implementation of changes to RISX-FACS®. The formally documented procedures include the process for regular changes, as well as the process for emergency changes. Changes to all platforms follow the same development and testing process (Control 4.01).

The change process begins with the request for a change. The change is initiated when an end user completes a request form located on the Gallagher Bassett intranet. After the change request form has been approved by the requestor's manager, it is sent to GBIT and loaded into a tracking system, called the Work Request System (WR System), for portfolio management tracking and review as well as other SDLC steps (Control 4.02). The WR System provides automatic email notification to all resources assigned based on Project Status and has the capability to store project documentation and project Move forms in a central repository. Work Requests are logged into Gallagher Bassett's tracking system and assigned a Work Request Number (WRN). These numbers are automatically assigned by the system. When the Work Request is entered, an automated email is sent to the requestor identifying the request and assigned number. Once entered into the WR System, an item becomes a part of the GBIT portfolio management and SDLC work flow process.

GBIT management reviews and prioritizes the change requests received. Change requests are reviewed and are labeled as an emergency change or as a regular change. Emergency changes are approved and moved to development for appropriate attention. Regular changes are prioritized for development assignment. The GBIT ADM team holds weekly meetings to discuss and review current status, goals, and any problems/issues. The Vice President of Applications Development & Maintenance monitors the status of ongoing development efforts.

Emergency changes are moved through the same procedures as a regularly scheduled release but typically have a higher priority. For those emergency changes where a workaround is possible, the project must be defined and addressed with appropriate attention (within two weeks). Emergency changes where a work-around is not possible are addressed with the highest priority (within 36 hours).

Demand Management

The GBIT Portfolio Management team manages and reviews portfolio items (i.e., planned IT changes) and addresses priorities and refinements as appropriate. After prioritization, both emergency and regular changes are forwarded to the proper Business Analysis team.

Business Analysis

The prioritized requests are further refined and elaborated by the Business Analyst group, part of the GBIT ADM team. The Business Analyst understands the business needs and provides detailed business requirements to the development and testing teams. These requirements are documented and approved by the respective teams before initiation of any development or testing efforts.

Development — Application and Database

When the development team receives the approved change request with the documented requirements, a programmer is assigned by his/her Team Lead to develop the change. The programmer's Team Lead works with the developer on understanding the requirements, design, and approach.

There are two separate testing environments in the Development (DV) System: one for testing (Programmer) and one for QA testing (Business System Analyst (BSA)). The programmer will copy the production version of the application(s) requiring the change(s) into a test region by executing TACL routine HP NonStop changes. Some of the changes will require changes to both RISX-FACS® Classic and .com/.net. Only the necessary application modules are copied into the testing (Programmer) environment (Control 4.03). When the changes are completed, the programmer will complete the Program Transfer Request form, fill out the Notify and Release Changes form (NARC, which details the changes and move requirements), gather the documentation related to the change, and submit the documentation to his/her manager. The Development Manager reviews the changes for adherence to standards and approves the changes by signing off on the Program Transfer Request form. All documentation is saved within the WR System and is given to the Program Administrator (PA), who will coordinate the move of the software to the QA/BSA environment. Automatic notification is sent to resources assigned to the project, informing them that the software is ready and/or has moved to QA for testing.

QA Testing

Once in the QA/BSA environment, the QA team will perform the Acceptance Test. If a defect is found in the test process, the QA resource will inform the developer, and the developer will pull the software back into the test (Programmer) environment to make any corrections. This is accomplished via a TACL routine (PROGBACK for HP NonStop). When the correction is made, the developer will stage the software to be moved back into the QA/BSA environment via a TACL routine (BACK2BSA for HP NonStop). The QA Analyst is notified and pulls the software back into the QA/BSA environment via a TACL routine (MOVE4BSA for HP NonStop) to continue testing. To validate that the QA/BSA environment has the latest version of the software, the QA Analyst and PA will execute a TACL routine (CHKB4LIV for HP NonStop) validating software versions. This TACL routine can be executed at any time during the testing cycle and is also executed before production migration. Changes can be made in only the testing (Programmer) environment (Control 4.03). Code is unable to be changed in production or the BSA/QA environment due to system restrictions. Typically, developers do not have access to production or BSA/QA, and an individual other than the developer will migrate the change into production (Control 4.06). However, in cases where duties cannot be fully segregated during an emergency change, a pre-authorized developer can move the changes into production, which will then be documented on the Move form. The Move form is monitored and reviewed for appropriateness by the Application Development and Maintenance group.

The size and/or complexity of the change will determine the level of user involvement in testing the change prior to movement to production. End users are notified when test items are available in the BSA/QA environment. The QA Analyst or Programmer may assist the user in testing, or the user may perform the testing. All Programmers' changes are tested by a QA Analyst. The QA Analyst will sign off on the Program Transfer Request form once completed with testing (Controls 4.04 and 4.07).

Production Moves — Application and Database

The QA Analyst sends an electronic copy of the NARC to designated areas/individuals as notice that a change has been approved. Subsequently, the QA Analyst's manager reviews the change(s) for adherence to standards, approves the changes (by signing the Program Transfer Request form), and forwards the project documentation and approval forms to the PA to migrate to production (Control 4.05). (Note: If the QA Analyst's manager reviews the change(s) and finds it does not adhere to standards, the change will not be approved to move to production and will be sent back for further development and/or testing.) The Work Request is updated to reflect that the project is Ready for Production. As a result of this update, the end user and all assigned resources are notified automatically when a system modification related to his/her request is being moved into production via the WR System. Notification allows the user to prepare for the production move, as well as allows the user to communicate, as appropriate, schedules and necessary information, such as new policies and procedures. The end user is responsible for user documentation and training. When changes are complete and ready for production, the PA reviews the request for move to production and reviews the Program Transfer Request form for completeness. If any additional production move preparation tasks are required, the project is forwarded to the appropriate personnel to complete those tasks. The GBIT manager, for each area involved in the production item being moved, signs off on the completed form. Once the request is returned to the PA and all affected areas have performed their duties, the program change(s) is ready to be moved to production. The PA reviews that sign-offs are complete and forwards the request to his/her supervisor. The supervisor validates that all of the appropriate sign-offs and notifications are completed (Control 4.05). The PA schedules the turnover by assembling the scheduled moves and any associated pending conversion scripts and forwards the request to Operations who migrate the change (Control 4.06).

Routine changes are moved the second and fourth Tuesday of the month; however, emergency changes may be moved into production outside of the typical change schedule. Emergency changes may present circumstances for special authorized access of development. Application moves and system-level (e.g., operating system, patches) changes will occur on the second and fourth Tuesday of the month. This production move schedule provides control and allows for identification of the root cause of any issues that may occur with a particular move. While every effort is made to remain on the second and fourth Tuesday of the month schedule, if the change is large and there is a risk of slowing the system down, or if there is a risk that problems with the migration would occur, or if users require the process to be effective on a specific date, the change may be scheduled to be moved over a weekend.

Once a successful migration is complete, the Operator signs off and returns the file transfer packet to the PA. The PA returns the file transfer packet to the Applications Manager, forwards a copy of the transfer request to the Applications Programmer, and files the original. The PA will update the Work Request to reflect that the project has moved to Production. An automated notification stating that the software has moved to production is sent to all resources identified in the Work Request for their records. The Applications Manager then closes out the change and any related material. The Work Request is updated to reflect that the project request has been resolved, and an automatic notification is sent to all resources for their records. The information is forwarded to GBIT administrative assistance to process the closed-out service request/WRN.

Operating System Changes

Changes to the operating system follow the process noted above, with the exception of the move to production, which follows the process in the Internet-Related, Operations, Monitoring, Maintenance, and Documentation section.

Other Information

System software, including Guardian and Safeguard, is purchased and not altered or enhanced by GBIT. Configuration changes to Safeguard are performed by GBIT and follow the above-stated change management process. The ability to perform configuration changes is restricted to appropriate personnel through system security. HP is contacted for system application problems (Control 4.08). In some situations, a patch may need to be applied. Any changes (including patches) are tested in a test environment (Control 4.03). If the new changes or a newly installed operating system does not work, GBIT falls back on the prior operating system. If no problems occur with the new version of Guardian (system software), it will be moved to production.

Internet-Related Operations, Monitoring, Maintenance, and Documentation

Web Servers

RISX-FACS® web servers run on Windows 2003 IIS 6.0 and are deployed in a load-balanced cluster for internet-facing traffic and a second load-balanced cluster for internal users. Traffic is filtered by a Cisco ASA firewall to only allow approved traffic to the web servers. Both the firewalls and load balancers are set up in a stateful automatic fail-over design. External web servers are deployed in a Gallagher Bassett Demilitarized Zone (DMZ).

The default installation is disabled, and the web user has minimal access to the system. The server does not allow directory listing or following of system links. In addition, the most recent operating system patches have been applied. A URL monitoring tool is used to detect any malicious or suspect activity on the web servers (including SQL injection attacks).

Only needed internet services are installed, and passwords are set up according to Gallagher Bassett standards (Control 5.04). These services are also made accessible to appropriate individuals (i.e., non-privileged users are not granted access to sensitive system utilities). Web server directory permissions are set such that the ability to upload files into web directories is allowed to any authorized person or sanctioned application (Control 5.05/Control 2.03). When possible, users are granted the ability to execute applications only within the parameters of the installed scripting engine. Some files (.dll and .exe files) or environments require users to execute applications on web servers. For those users, execute permissions have been granted both at the file system level and at the web server level. Web directory browsing is deactivated on the web servers. Also, the administration website, which allows for remote administration of the web servers, is disabled. If the website is not highly sensitive, remote administration may be enabled, but only administrator Internet Protocol (IP) addresses are allowed to access the website.

Changes to the web servers are tracked and approved through BMC (REMEDY) Change Management (Control 5.02). Changes are initiated using BMC (REMEDY) Change Management. The requestor is alerted when the request has been either approved or rejected. Once the change is completed, the change record is marked with the completion date. Critical changes are immediately implemented with an entry in BMC (REMEDY) Change Management. After implementation of the critical change, an entry is made in BMC (REMEDY) Change Management with the date required for the change marked as “Emergency.”

Regular, vendor-supplied operating system patches are considered routine changes and are not subject to the process described in the preceding paragraph. These patches are applied monthly. If a critical level operating system patch is introduced by the vendor during a period, action is taken to review and deploy immediately as appropriate.

Firewalls, Routers, and Network Monitoring Tools

The firewalls and routers are maintained by authorized Gallagher Technology Services employees. Cisco ASA firewalls are used between the Internet/DMZ and DMZ/Inside. Using ASAs, redundant firewalls are able to sync the same configuration file. Changes to firewall configurations and routers (Control 5.02) follow the same policies and procedures as changes to the web servers. Once the change is completed, the change record is marked with the completion date.

Implementation Data Services (IDS) monitors the DMZ web server sub-net and logs events for review. If a potential service is detected, an alert will be sent to the LAN administrator who will investigate and resolve the problem (Control 5.03).

SSL

Gallagher Bassett uses the secure sockets layer (SSL) when transferring information between the user and the Load Balancer (Control 5.01). When a user logs on to www.RISXFACS.com®, after 10 seconds or upon clicking on the globe on the main page, a secure session is established with the server. The private key is maintained by the Gallagher Technology Services Department and provides 128-bit encryption.

Monitoring

A vulnerability security scanner is used by Gallagher Technology Services on a weekly basis to scan RISX-FACS computer systems to assess any potential security risks. As appropriate, security vulnerabilities detected will be addressed by the Global IT security team by patching the Windows System via Microsoft SCCM.

Log-on attempts to RISX-FACS.com® are logged in a security management tool's secure log. Any failed attempts go into a failed log (sys log) that is stored on a separate server. The log is monitored at least once a week by the Gallagher Bassett security team (Control 5.03). If a data breach is suspected, Gallagher Bassett follows procedures within the Corporate IT Policy for Security Incident Management. Network routers and switches are logged to a central syslog server for review in case of an incident.

The website is monitored 24/7 for uptime via the Microsoft System Center Operations Manager — SCOM. Network hardware is monitored 24/7 for failure via Simple Network Management Protocol (SNMP) monitoring.

Claims Processing

Claims Setup Procedures

Claims processing is initiated through loss notification. Notification of a loss may be received via fax, mail, electronic data interchange (EDI), or telephone. If received by telephone, fax, or mail, the loss will be manually set up in RISX-FACS® by Gallagher Bassett. If the loss is received by EDI, it is automatically entered into RISX-FACS®. The initial notification is considered the notice of loss. The claim is to be set up within RISX-FACS® based on the loss report submitted to Gallagher Bassett (Control 6.01).

Once the initial accident screen is complete, RISX-FACS® may bring up a screen listing other accidents for the applicable client. RISX-FACS® will indicate if the current accident may be a duplicate (Control 6.02). The processor reviews and determines whether a duplicate accident exists. If the processor determines that the accident information has been previously entered into the system, the processor will add the claim to the existing accident, rather than creating a new accident record. For new claims, RISX-FACS® automatically generates a 16-digit claim number based on the client code.

The processor contacts the appropriate party to ascertain the claim validity and facts (Control 6.05). The contacts required are dependent on the type of claim. There are three types of claims services lines: workers' compensation, liability, and property. Workers' compensation is divided into two service lines: indemnity and medical-only. Indemnity or medical-only converted to indemnity claims require three-point contact (client, claimant, doctor); liability claims require two-point contact (client, claimant); property claims require one-point contact (client); and medical-only claims do not require contact (unless specified in the CSI). This contact is made and documented in the Claim Notes screen in RISX-FACS®. Investigation of the claim is evidenced in the Claim Notes screen in RISX-FACS®. For claims requiring contact, 24 hours within receipt is considered timely, unless otherwise specified in the CSI.

Supervisors perform a claim setup review on all claims types, except medical-only (Control 6.03). The claim setup review is considered to be performed in a timely manner if it occurs within 30 days. A Supervisory Note is added to the claim (as noted above) addressing appropriate contacts, data integrity, initial reserves (Control 6.04), and Plan of Action. Data integrity controls include all coding applicable to the facts of the claim and, in addition, any client-specific coding as outlined in the CSI. The Plan of Action, which is completed by the adjuster, is used to summarize the claim file's current status and outline future steps needed on an individual file. The Plan of Action may also include (but is not limited to) the following categories, depending on the line of coverage: Supervisory Comments, Coverage, Reserves, Injuries/Damages, Subrogation, Litigation, and Settlement Information.

Subsequent supervisory reviews are performed at least every 100 days after initial claim review setup, unless otherwise stated in the CSI, to help ensure a Plan of Action is in place and reserves are appropriate based on facts known to date (Control 6.06). As part of the review, the supervisor will provide claims handling guidance, as well as ask the adjuster to complete any item that the supervisor may determine needs to be updated. There are claims that will close before 100 days, which are considered "fast-track claims," and they do not require a subsequent supervisory review. These fast track claims are generally medical-only workers' compensation claims or minor claims in the following lines of coverage: workers' compensation indemnity, auto property damage, property, and auto/general liability claims.

If a claim is reopened, the supervisor will perform an initial review within 30 days of reopening and every 100 days thereafter while the claim remains open.

Supervisors and adjuster diaries are set according to Gallagher Bassett standards at a frequency not to exceed 90 days. The frequency of the adjuster and supervisor diaries may be less than 90 days, depending on the nature of the claim. In order to monitor compliance with Gallagher Bassett standards and escalate out-of-compliance claims, supervisory diary compliance reports are generated monthly and sent to the Branch Manager's attention with details of any claim that has not been reviewed within 90 days of the report date. The Branch Managers then provide the detailed list of files to the supervisors to review the out-of-compliance files and the files approaching the compliance due date.

Any communications regarding the claim and changes in the claim status are documented in the Claim Notes screen in RISX-FACS®. The claim notes are updated based on Gallagher Bassett standards, unless otherwise stated in the CSI. Based on the diary frequency coded into the system, the adjuster and supervisor receive diaries in order to review the claim status. There is also a special diary that allows the adjuster or supervisor to receive system reminders to perform claim status reviews.

The reserve amount set by the processor is dependent upon the evidence of the case and the type of claim. For workers' compensation claims, Gallagher Bassett estimates the reserve amount based on prior experience and factual evidence of the case. For liability claims, the reserve amount is determined based on the injury and percentage of liability. For property claims, the reserve amount is determined based on the damages and applicable coverages. Reserve breakdowns appear in the Claim Notes screen in RISX-FACS®. RISX-FACS® will not allow an adjustment of reserves reaching a total experience of $5,000 for a workers' compensation claim without the adjuster completing a Total Experience Worksheet, which is a detailed breakdown of the reserves (Control 6.08). Changes in reserve amounts are communicated to client personnel based on thresholds specified in the CSI. If stipulated in the CSI, Gallagher Bassett obtains authorization from client personnel to adjust the reserve amount over specified thresholds (Control 6.07).

Controlled Loss Reporting

Branch management must be notified of claims in which the self-insurance retention (SIR) threshold is met or exceeded (typically 50% of the SIR) or severity triggers are met. This is necessary, as the insurance carrier must be notified when its layer of coverage may be penetrated. A loss management report is sent on a daily basis to branch management, who track for completion of the appropriate carrier notification. A controlled loss report is sent on a monthly basis to branch management (Control 6.09). The controlled loss report aggregates all claims that were triggered in the previous month. In the report, each branch reported the actions taken on the controlled losses to upper management on a monthly basis. The process is centralized within the GB Service Center, which has the responsibility to complete the monthly controlled loss report from branch management (Control 6.09). The actions taken for each claim are documented in the monthly report and stored on a GB shared services site for branch and upper management review.

Payment Processing

RISX-FACS® Check Issuance

The appropriate damage factor is required in order for the RISX-FACS® user to set up a payment. Whether the payment is a one-time payment or a repetitive payment, the payee and mail-to information must be entered by the adjuster. If a payment is not being paid to the "other" category, RISX-FACS® does not allow the adjuster to change the payee name. Payments that are made to "other" would be any payment that is not made to the claimant or the client. If the adjuster selects mail to claimant, he/she cannot change the address. If the other payment category is chosen, the user manually enters a Tax ID number and is taken to a provider listing. Here the user chooses the correct provider, and the name and address information is automatically populated into the "payee" and "mail-to" data fields. The coding of the payment corresponds to the payee and/or the type of provider they are or the service they are rendering. Gallagher Bassett utilizes coverage-specific pay codes that break down the payment to notate the provider type or service rendered. As further validation, Gallagher Bassett compares the pay code selected against the provider file that has been established to help ensure that the pay code corresponds to the provider file setup of medical (M) providers or Non-Employee Compensation (NEC) providers. The provider file has a flag that indicates the difference between an M and an NEC provider, such as a lawyer or an auto shop. Any medical payments must be attached to a provider where the flag is set to M (indicating a medical provider). If a provider is not located in the provider listing, the adjuster adds the provider and appropriate information.

Gallagher Bassett has the ability to issue payments in a variety of currencies via a Citibank product called WorldLink. If a non-USD payment is needed, a request will be made to CFS by the adjuster via Lotus Notes. CFS inputs the payment into WorldLink and releases a check on a weekly basis. A static payment is entered within RISX-FACS® to record the transaction.

RISX-FACS® requires the payment breakdown to equal the check amount as a validity check. If the sum of the payment breakdown and the check amount entered are not identical, RISX-FACS® will not allow the payment to be entered into the system (Control 7.03). RISX-FACS® also prevents the adjuster from making a payment in excess of the amount remaining in the corresponding total reserve or expense category (Control 7.04). In order to make such a payment, the corresponding reserve or expense category must be adjusted by the processor to meet or exceed the payment amount. Supervisors review claims, and thus, would be aware of changes in reserves and payment amounts.

Stop Pay Issuance

Stop pays are checks that have been issued and sent out but need to be voided (e.g., lost in mail, wrong address, wrong amount, or duplicate payment). Stop pays as coded in RISX-FACS® include both canceled checks and stop payments. A stop pay is placed on a canceled check typically because a check was returned to Gallagher Bassett. The check is retained within the claim file, and the signature line is removed by the check handler. A stop pay is placed on a check typically because a check was lost in the mail or, prior to delivery of the check, a discrepancy was noted with that check. Adjusters and/or Claim Assistants are made aware of these stop pays verbally from the claimant or service provider. Authorized branch personnel contact the corporate home office to request a stop pay and provide reasoning for the stop pay and the date requested. The stop pay can only be requested due to claimant or service provider request. When the form is submitted to the corporate home office, a copy of the confirmation is printed for the file.

The corporate home office processes the stop pay on the bank's website based upon the information provided by domestic branch locations. Nightly stop-pay transmissions from Citibank N.A. (for Citibank U.S. bank accounts) are received showing what has been stopped for the day. This transmission is fed into RISX-FACS® and matched to issued checks. The checks that are matched to the transmission are marked as "stop paid" in RISX-FACS® (Control 7.11). Within approximately 24 hours, branch adjusters are able to view the status of the stopped check online. The category of the check then changes from issued to stop paid. A check reissue cannot occur until the original check's status appears as stop pay in RISX-FACS®. To stop pay a check issued from Citibank Canadian bank accounts, a request is sent from the adjuster to CFS to place a "stop pay" on a particular check. CFS then emails the following information to the Canadian branch of Citibank N.A. to verify if the check is still outstanding: (1) check number, (2) check date, (3) amount, and (4) account number. If the check is outstanding, a stop-pay form is emailed to the Citibank N.A. Canadian branch. After the branch confirms the check has been stopped, the check is stopped in RISX-FACS® (Control 7.11). CFS then emails notification of the stop payment to the adjuster, and the transaction is noted for reconciliation purposes.

Payment Authorization

Claim payments in excess of $50,000, unless specified differently in the client service instructions, must be authorized by the payment authorizer for that location (Control 7.01). RISX-FACS® does not allow payments that have not been authorized to be sent to banking for issuance. Unauthorized payments are placed in a "hold" status (Control 7.02). These checks cannot be released until the proper approval(s) is (are) received. Approval must be granted from the payment authorizer setup within RISX-FACS®, which could be the branch manager or client. The authorization may be set up at two levels within RISX-FACS®:

- **Initial Authorization** — This first authorization level encountered for payments is optional. When set up, it is granted to individuals such as a branch manager (or designee) or client. The authority level may be set from $1 up through $49,999. If no Initial Authorization is set up in the system (which is common for U.S. operations), all payments must be authorized through the second type of authorization, Final Authorization.

- **Final Authorization** — This second authorization encountered for payments is always activated. When set up, it is granted to individuals such as a branch manager (or designee) or client. Although the authority level may be set to a different amount, the final authority is generally for amounts in excess of $50,000. Final Authorization is the only authorization required in the absence of Initial Authorization.

Payment Authorization Monitoring Activities

Prior to November 2012, a report of payments in excess of $50,000 detailing who authorized the payment is printed and reviewed once a month. This report is reviewed to determine that the authorizer is neither the adjuster nor the issuer of payment. If any such instances occur, the Operational Security Administrator (OSA) notifies the Branch Manager via email and requests that he/she review the process with the appropriate party. The Branch Manager will then review the process with the appropriate party to ensure that established standards and procedures are being adhered to. Beginning in November 2012, the report of payments in excess of $50,000 is reviewed daily by the Gallagher Bassett Service Center (GBSC). Please refer to the Legitimate Payees section, as this control is part of anti-fraud report review (refer to Control 7.12).

e-Box Bill and Invoice Processing

Note: The following processes relating to the e-Box, e-Bill, and e-Invoices do not apply to Canadian managed accounts, as they do not process medical bills.

The claims imaging service organization, Coventry, sends files to Gallagher Bassett daily containing medical bills and medical reports that have been scanned and are ready for processing. Included with the transmission is a separate file of the images of the items scanned. Currently, HCFA, UB92 (standard forms used by hospitals and providers used to detail their provided services), and nonstandard forms are being scanned. This includes correspondence that is attached to a bill. Correspondence received independent of a bill is not scanned and is sent to the appropriate branch for processing. Jopari is an e-bill clearing house for medical bills. Jopari sends scanned medical bill files to Gallagher Bassett, which then in turn approves the bills. After approving them, Gallagher Bassett passes along the approved bills to Coventry for repricing.

A program created by GBIT reads the files and passes the claims through a series of edits, such as searching for an associated Tax ID number and claimant name against the provider and subscriber files. Medical bills not passing the edits are rejected and automatically returned to the medical provider by the system. Medical bills that have passed the GBIT program edits are separated by branch and adjuster and loaded into the adjuster's e-Box. In addition, RISX-FACS® automatically checks for duplicate payments and provides the adjuster with a listing of possible duplicates (Control 7.08). The listing can be displayed within RISX-FACS® for the adjuster to review prior to making a payment. Adjusters may reject payment if the potential duplicates correlate with the payment billed on the corresponding e-Bill or e-Invoice.

e-Bills

e-Bills are bills from medical providers relating mostly to domestic workers' compensation claims. Some U.S. liability bills may be sent via e-bill as a practical matter, but most e-bills relate to domestic U.S. workers' compensation claims. Adjusters log in to their e-Box and select the e-Bill icon. The adjuster can view the contents of the e-Box (new e-Bills, e-Bills in hold status, etc.). e-Box is an electronic inbox for individual adjusters where electronic claims (e-Bills) needing to be processed are presented to the adjuster. The adjuster selects an e-Bill and views the claim and billing information. The adjuster can view the image of the bill, search the provider files, or print the detail of the bill. The adjuster compares the image of the bill to the information displayed by RISX-FACS® to validate that the bill belongs to the claim. In addition, the adjuster reviews the bill and checks for reasonableness. If the bill does not relate to the claim on file, payment is not made by the adjuster. If the adjuster is not able to substantiate or match the e-Bill and/or e-Invoice to the vendor bill image for e-Bill and by claim documentation for e-Invoice, the e-Bill and/or e-Invoice are rejected (Control 7.09).

The adjuster has the authority to perform the following options related to the bill:

- **Reject Bill** — Adjuster could reject bill if a medical report is not included, claim is voided, client is terminated, there are duplicate charges, etc.
- **Do Not Pay With Review** — Adjuster would send the bill to the managed care provider without paying the bill (in order to see what the repriced amount would be).

- **Pay Bill, No Review** — Adjuster would pay/accept the bill without managed care review (e.g., prescriptions).
- **Pay Bill With Review** — Adjuster pays/accepts bill and sends to the managed care provider for repricing/review.
- **Reassign Claim** — If bill is associated with the wrong claim, the adjuster can reassign the bill to the correct claim number for that claim's adjuster to process as appropriate following these procedures.
- **Do Not Pay, Hold Status** — Adjuster would place bill on hold if additional research is needed to be performed or if the client needed to be contacted, etc.

Once the adjuster selects a bill option, RISX-FACS® displays a dialogue box indicating the status of the e-Bill. Built-in edits and validation routines prompt the adjuster to review for duplicate e-Bills (Control 7.13) when the Pay Bill, No Review option is selected; and automatically populate the claim notes under notebook subject "002" with the bill options selected.

e-Invoices

e-Invoices are bills for case management charges, hospital pre-certification charges, prescription charges, etc., relating to associated claims. Adjusters log in to their e-Box and select the e-Invoice icon. The adjuster can view the contents of the e-Box (new e-Invoices, e-Invoices in hold status, etc.). The adjuster selects an e-Invoice and views the claim and invoice information for the selected item.

The adjuster has the option to perform a check for duplicate payments, print the detail of the invoice, and accept or reject the invoice. Invoices include a progress report where appropriate. The adjuster reviews the progress report, bill, and charges for reasonableness. If the charges are reasonable and related to the associated claim, the adjuster accepts/pays the charges. The adjuster rejects an invoice if there is not a supporting progress report, if the invoice is for an injury not related to the claim, or for any other reason documented in RISX-FACS® (Control 7.09).

Manual Invoices/Bills

Invoices or bills received in the branch require that payments be processed manually (refer to controls listed above for Payment Processing). Manual bills will be reviewed in a similar manner as e-Bills or e-Invoices. The adjuster will review the bill to validate that it is related to the claim, the charges are reasonable, and the provider is valid. Once validated, the adjuster will verify appropriate reserves are in place, identify the claim number, apply the appropriate pay code, and note their approval. The invoice/bill will then be placed in line for check issuance through RISX-FACS®. Once paid, the bill will be placed in the claim file. The Canadian branch receives only manual bills.

Claim Checks and Client Correspondence

Each night during the batch run, temporary files are created in RISX-FACS® containing the processed check and correspondence information for that day. These temporary files are automatically downloaded to a server in the data center. The temporary files contain a header and trailer record. The header record identifies the file. The trailer record gives the total check count and dollar count included in the file. These files are referred to as the Claimant and Provider files, which are sent to MicroDynamics, a third-party service vendor, for check printing, and Citibank N.A. for the Positive Pay framework utilized for Citibank U.S. bank accounts. In addition, five files are created and sent via encrypted file transfer protocol (FTP) to a banking source as a single file. The five files are as follows:

- Citibank N.A. checks (U.S. and Canadian Citibank bank accounts) to be printed at Citibank N.A.
- Citibank N.A. (U.S. and Canadian Citibank bank accounts) checks printed at another vendor
- Non-Citibank checks to be printed at Citibank N.A.

- Electronic funds transfer (EFTs) with advice
- EFTs without advice

The banking source is called to validate receipt, and an email is generated, which is sent to Gallagher Bassett Operations.

The header information is embedded in the record that represents each payment. Each record contains 31 bytes of claim information:

- Form name
- Flag designating if the form is a check or correspondence
- Dollar amount (blank if correspondence)
- Block Identification Number (BIN) or document number
- Additional instructions and/or information: mailing specifications (FedEx or UPS), type of form to be used, alignment, etc.
- Batch instructions (all pieces to the same mailing address are bundled together for postage savings)

Notification is provided via the message log, stating that Claimant and Provider files are complete. An Obey file for Claimants and Providers is executed, and files are sent via an internal transfer process to a local server where the MicroDynamics Group files are encrypted and sent to the MicroDynamics Group. The second set of files is encrypted and sent directly to Citibank N.A. for processing.

Print screens of the banking totals are attached to the banking packet and stored.

The computer operator receives an email from the check-printing service containing the dollar amount, total number of forms, and total number of checks. The computer operator verifies that they match the same totals produced from RISX-FACS® (Control 7.05). This reconciliation also validates that the bytes sent to the check-printing service were the bytes received by the check-printing service. For EFT, the Operations staff receives an email from the banking service containing the total number of EFTs and the total dollar amount of EFTs (with and without advice) and verifies totals produced from RISX-FACS®. The computer operator validates the verification on the check-printing service's control form (Control 7.06). The control form, the BKQ15, and the fax from the check-printing service are routed to the Supervisor, who double-checks that all steps in the banking reconciliation packet were completed, including the verification of balancing totals, by completing the Daily First Shift Banking Checklist (Control 7.07). The forms are retained for one year. The process is performed every night except Saturday, and always on the last 2 days of the month to satisfy month-end financial reporting requirements.

Generally, all checks are printed and mailed directly from the check-printing service's facility on the same day in which the check-printing service receives the file from GBIT. RISX-FACS® does have the capability to allow for printed checks to be issued and mailed back to the branch for mailing from the branch. In addition, CFS may submit special requests for check pulls if a check needs to be sent overnight rather than through traditional mail. To request that a printed check be pulled and returned to the requester, a Gallagher Pull Request form must be completed and signed by the requester and faxed to the Account Administrator at the check-printing service. This fax is followed by a phone call to the Account Administrator. The Account Administrator will have the items identified on the check request pulled and sent overnight to the original requester.

Field Pays

Field pays are manual checks that are issued at a local branch for payment rather than a computer-generated check processed through RISX-FACS®. All domestic claim branches have field pay check stock but may not necessarily need to use it. The Canada branch does not have the ability to process field payments, as they are not provided physical check stock. Field pays can occur on any claim and normally occur for case settlements or rush payments to contractors. Other examples of when they occur are when there is an issue, such as settlement of a case with legal counsel, which requires a payment to be received by a payee in less than two days. A check processed through RISX-FACS® will not reach the payee in time; therefore, a manual check is issued and sent by overnight delivery to the payee.

The manual checks are maintained in a folder in a locked cabinet. Only designated branch personnel have the keys to this cabinet (Control 8.01). Issued, voided, and unused checks are recorded and tracked in a field payment log (Control 8.02). This log is examined by the designated reconciler each month (Controls 8.01 and 8.03). Manual checks are requested from the Accounting Department in Itasca, Illinois, when the stock runs low. The quantity of stock is dependent upon each branch's usage. Manual checks are not allowed to be left at a clerk's desk while being issued. The clerk must either complete the check issuance process or store the check and corresponding documentation in the check stock folder until completion can occur. Field payments can only be issued for clients that use the AJG omnibus account. If a client has chosen another type of banking, Gallagher Bassett cannot issue a field payment on their behalf because the check stock with the client's account number on it is not provided to Gallagher Bassett. There are a few exceptions where the client has provided check stock to the branch; however, it is typically on older claims. Gallagher Bassett does not encourage this practice. However, if client check stock is used, the same handling rules (as if for the AJG omnibus account) apply.

The adjuster determines if a field pay is necessary and requests a field pay check from the custodian, who will process the request. The next available check is taken from the check stock envelope by the custodian. The check is completed and then entered on the check payment screen in RISX-FACS® based on the field pay instructions, with the code of "F" entered to designate field pay. RISX-FACS® supplies a voucher number for the transaction. This voucher number is entered in the field pay log book. Once complete, the check and related information are given to an authorized signer at the branch. Only authorized branch personnel can sign the field pay check for issuance to the payee (Control 8.04). The check must be entered into RISX-FACS® before the check can be signed; a copy of the signed check and initialed RISX-FACS® screen must be placed in the claim file. Completed field pays are sent out to the payee via FedEx or UPS, or the payee may come to the office to pick up the check.

Check Handling

Checks that are received in the mail are not handled by branch adjusters. During the mail process, checks are separated from the other mail, and all envelopes/correspondence are kept with the check. The original check is photocopied onto lime-colored paper, and the photocopy is given to the adjuster. The original checks are handled by only the designated check handler at the branch (Control 8.05).

Field Pay Monitoring Activities

The VP of Risk Management monitors authorized signers at each branch. A list is maintained and updated by the VP of Risk Management. The standard is two authorized signers per branch, although some larger branches may have more than two. Reports listing all field pay checks by branch are emailed to the Branch Managers once a month for review. The report is reviewed against the field payment log book to ascertain that all checks have been documented appropriately. All discrepancies are reported to Risk Management. Risk Management then follows up to resolve any issue reported. The reconciler reviews the field payment folder to ascertain that unused checks are in the folder. The reconciler then signs off on the log, indicating the completion of the review.

Legitimate Payees

RISX-FACS® users with check issuance capability are allowed to set up claims, authorize payments, and specify payees for payment. These claims processing functions are allowed to be performed by each individual in order to maximize productivity.

On 1 November 2012, GB deployed the use of advanced data analytics as the primary control for fraud detection monitoring of daily claim payments. GB uses specialized software called Audit Command Language (ACL) for the claim payment analysis. ACL is recognized worldwide as the leading stand-alone data analytics software for audit, financial, risk management, and compliance professionals.

The VP of Risk Management initiates the daily production of 30 antifraud reports focused on internal and external fraud detection. The data feeds include all daily manual claim payments, managed care payments, EFT payments, and claim reserve changes. The 30 exception reports are uniquely programmed for a specific fraud risk scenario and scheme. All report exceptions are reviewed by the GBSC (Control 7.12). Unresolved or unexplained payment transactions are referred to the appropriate Branch Manager for confirmation of payment validity.

Every six months, a report is run listing dollar amounts paid out to surveillance/investigative and medical case management providers. The report is broken down by branch, adjuster, managed care provider, and claim number by adjuster. This report is examined by the Senior Vice Presidents and Vice Presidents for any unusual amounts paid out and trends that may be occurring (Controls 7.10 and 7.12). Anomalies are reported to the VP of Risk Management for further investigation.

The system searches for possible duplicate e-Bills based on a certain set of criteria. On a monthly basis, a report is sent to each managed care provider identifying the possible duplicates. The provider must respond to each possible duplicate and take the appropriate action via email.

Recoveries Processing

Recoveries Processing

Recoveries are funds that have previously been paid off of a claim file and are being refunded back to Gallagher Bassett for a variety of reasons. When a recovery is refunded to Gallagher Bassett, it is first sent to the claims-handling branch office. At the branch, the type of recovery that is refunded is identified. Recoveries are classified as follows:

- **Subrogation** — Collection of monies from responsible party
- **Salvage** — Refunded value of a damaged piece of equipment
- **State Fund** — Reimbursement from a state where injured rehired workers' benefits are supplemented by the state
- **Other** — Category that is most widely used, covering reimbursements due to overpayments or reconsideration of bills from providers and claimants

Excess recoveries occur when claims paid for a particular claimant go beyond the level agreed to be paid out by the client before being paid by an excess carrier. With a recovery related to claim payments extending into the excess layer, the collection process is initiated with the carrier according to the specific carrier instructions. Adjusters do not process excess recoveries. The excess carrier reimburses the client through Gallagher Bassett for those monies in excess as agreed upon and according to specific carrier instructions. Recovery information is then prepared by Gallagher Bassett detailing the claim number, the amount paid out by category (e.g., medical, expenses), and the amount when the excess layer becomes effective. This information is usually documented in a Specific Excess Recovery Document (SERD) but may be in the form of an email or other communication. This information is sent to the corporate home office for application of the recovery check, which includes entering information into RISX-FACS® (Control 9.04).

Prior to the processing of a recovery check, a Check Processing document is completed by the adjuster. This document is then passed on to the clerical staff for inputting into RISX-FACS®. The clerical staff enters the pertinent information into RISX-FACS® (e.g., claim number, claimant name, check number, check date, check issue, recovery type, and reason for recovery). Upon completion, a system-generated recovery voucher is printed. The branch office then attaches the recovery check to the voucher. The branch then scans this document, attaches it to the claim notes, and mails the original check and voucher to the Recovery Unit for processing.

An automated process handles large managed care provider recovery batches. These recoveries relate to rate changes, billing coding errors, etc. Once an incident is identified, Gallagher Bassett works with the provider to get a data file of the recoveries, which can be uploaded directly into RISX-FACS® (Control 9.03). These batches are outside of the manual recovery process and do not produce system-generated recovery vouchers.

All information related to the recovery is entered into RISX-FACS®. CFS reviews for accuracy. If differences are noted between the recovery voucher and the supplied backup (such as check number, check date, or check issuer), CFS will make the necessary changes before processing the recovery (Control 9.01).

CFS determines if it is a direct deposit or endorse and mail recovery. Direct deposit recoveries are recoveries that Gallagher Bassett can deposit into the Self Insured Money Management System (SIMMS), a Citibank escrow account. Endorse and mail recoveries exist for clients who select the voucher or Client Owned Banking (COB) method. In these instances, Gallagher Bassett does not have access to the bank accounts and, therefore, cannot deposit the recovery. Gallagher Bassett will then endorse the check and mail to the address specified within RISX-FACS®.

CFS has the ability to create recovery vouchers if checks are sent directly to them rather than to the branch or if a voucher must be voided and re-entered. The Recovery Unit of CFS, upon receiving vouchers and checks, validates information and posts recoveries to the claim file (Control 9.01).

CFS or the Accounting Department then either applies the money to the appropriate account or endorses the check to the proper party and mails it. Money can only be applied to Citibank N.A. accounts (Control 9.02). Therefore, checks must be mailed to clients not having a Citibank account (Control 9.02). In addition, recovery checks, for clients that have Citibank accounts, may be prohibited from being direct deposited due to any of the following reasons:

- The client has a voucher payment system established
- The client resides in a state that prohibits monies from being held outside the state

Recoveries applied to Citibank accounts are sent to Citibank via FedEx each night for next-day deposit (Control 9.02). Standard letters may be sent to the proper party giving the details of the transaction, if required by the client. Otherwise, clients are notified of recoveries via RISX-FACS® recovery alerts that are set up and maintained by the appropriate Account Manager.

Client Reporting

Report Setup and Maintenance

Client reports may be requested to be received at a specific frequency (e.g., monthly, semimonthly, quarterly, or annually) for an additional fee. Reports may be received via four different types of media: email, internet (RISX-FACS®), CD-ROM, and/or paper (simplex or duplex, i.e., front or front and back) (Control 10.01). There is a standard set of reports that includes the following: Activity Summary, Claim Activity, Claim Register, Loss and Claim Experience, Specific Excess Loss Report, Summary Loss Report, Claim Loss Analysis Report, and Accident Loss Analysis Report. The default for most standard reports is via the internet (RISX-FACS®) and is provided monthly or annually, depending on the report. The recipient determines what reports are received, as well as when they are received.

For new clients, reports are initially set up when the initial loss program is set up in RISX-FACS®. Reports are set up based on requests from the Account Manager, Producer, per the carrier requirements, or for internal users for special reporting purposes. Special reports such as the Detailed Status Reports (DSRs) are user-requested through the Account Manager via the Notice of Sale, from Costing & Quoting (Control 10.02). In addition, any changes in frequency and media must be requested through the Account Manager or internal recipient.

Implementation and Data Services is responsible for maintaining the Report Distribution Maintenance screens and the recipient lists in RISX-FACS®. The Report Distribution Maintenance screens provide the report preferences, the media (email, internet, paper), and the contact information for each recipient and loss program setup for each client. Recipient codes are entered into the system in order to tie the client reports to the appropriate contacts. Recipient numbers 0001 through 0010 are automatically assigned by RISX-FACS® during the setup process for each client; any additional recipients can be added or deleted per client request.

Report Processing and Distribution

Report Processing

Automated system checks comparing previous month totals plus current period activity validate that reports are in balance. When reports are out of balance, an error message is generated and email notification is sent to appropriate members within CFS, IDS, and Operations (Control 10.03). The report is placed on hold until the out of balance is resolved.

Hard Copies (Paper) or CD-ROM — Operations

Report printing is initiated in the corporate home office, but the actual printing and distribution are performed by a laser printing vendor (MicroDynamics Group). Automated system checks within RISX-FACS® validate that report distribution processes are completed in a timely manner without error. The RISX-FACS® system generates and stores the client report information and generates two copies of a register sheet. The register sheet is a listing of the reports generated for each client. One copy of the register sheet is retained by Operations. The Operations group records the total number of clients the reports are generated for and the total number of recipients of the reports (i.e., one client could have multiple recipients of the report) onto the Report/Distribution Log. The reports are sent to the laser printing vendor electronically via a secured circuit. The other copy of the register sheet is sent via mail to the laser printing vendor.

The vendor maintains a log of reports distributed for Gallagher Bassett and provides confirmation that all reports for the processing period have been sent. Gallagher Bassett receives this log daily until all monthly reports have been distributed. Operations records the report ship date for each client onto the Report/Distribution Log. A reconciliation between Gallagher Bassett and the report printing vendor is performed monthly. Any variances between the number of reports generated versus the number of reports actually shipped by MicroDynamics Group is investigated by Operations (Control 10.05).

Electronic

Clients can opt to receive their reports via email or RISX-FACS® online. Recipient lists are maintained the same as with paper reports; the only difference with the email format is that when the reports are created, the output is not to a file but is emailed based on the distribution list. A job containing automatic system checks is run to validate that all email reports have been distributed and are in balance (Control 10.04). Rejected report emails are sent back to an inbox that is monitored by IDS. IDS ascertains that the email address is correct and the contact information is updated. RISX-FACS® includes a utility that allows Gallagher Bassett to reship monthly reports via email, if necessary.

The Operations Department executes an automated process to create and securely transfer a file to an internal server administered by the AJG Shared Services LAN Department. A separate job is run containing automatic system checks validating that internet reports have been distributed and are in balance. Once set up with the proper security on RISX-FACS®, clients can navigate to the Gallagher Bassett website and view their reports online.

Cash Management

There are three banking methods available to Gallagher Bassett clients:

- COB
- Voucher
- SIMMS

COB

With COB, the client gives Gallagher Bassett the authority to write claims checks from the client's checking account, but Gallagher Bassett does not have access to the client's banking information, such as bank balances or funding mechanism. Gallagher Bassett sends the checks to be printed by an outside check-printing service provider, MicroDynamics Group. The checks look like a Gallagher Bassett check but with a different account number, and the client's logo is imprinted on the check.

Voucher

Voucher banking involves the issuance of a payment authorization (voucher) document in lieu of a check. The voucher is mailed to the corresponding client, instructing the client to make the payment(s) to the designated payee(s). The voucher contains all relevant claim-related information. With voucher banking, Gallagher Bassett provides the claim handling service, and the client handles the issuance of payments.

SIMMS

SIMMS refers to a controlled disbursement product developed and used in conjunction with Citibank N.A. SIMMS, together with the Automated Payment and Control System (APACS), a RISX-FACS® application, provides the mechanism that allows Gallagher Bassett to issue and clear large volumes of checks through a single omnibus account at Citibank N.A. SIMMS provides the ability to attach sub-accounts to the omnibus account for separate and distinct client banking arrangements. This feature is the single most important element of SIMMS. The client sub-account holds the client imprest (working funds) and will ultimately receive credit and debit activity. To initially establish the account, paid loss history is used to calculate the required imprest. A banking parameter agreement is signed by the client. The agreement specifies the sub-account number, imprest amount, and frequency and method of funding (Control 11.01). A copy of this document is maintained in the banking folder on-site. Typically, clients will fund the sub-account based on checks that have cleared the account. On occasion, a client may fund the account based on issued checks.

SIMMS relies on a daily transmission file (issuance file) from Gallagher Bassett to Citibank N.A. The file contains issued payment specifics, including plan number, check number, payment amount, etc. Citibank uses this information to identify and pay checks that are presented for clearing. A positive-pay system is used to pay only those checks that have a matching issuance record in RISX-FACS®. The match-paid checks are then debited to the client's sub-account. Within 24 hours, a "cleared payment" transmission is received by Gallagher Bassett from Citibank identifying those checks that have been match-paid. This file is used to update RISX-FACS® with the payment clear date. Based on the prescribed funding schedule, replenishment is requested, the sub-account is funded, and the cycle is complete.

If a check does not match an existing issuance record, Citibank contacts Gallagher Bassett. Gallagher Bassett investigates the item and issues a pay, no-pay instruction via an online connection (CitiCash Manager). Otherwise, Gallagher Bassett resolves the matter with a branch or via corrective input to RISX-FACS®. This process is not applicable to Canadian bank accounts, as GB does not have an omnibus account established to manage these bank accounts. Each client account is managed manually on an individual basis.

CFS downloads debit and credit information from Citibank N.A. and Citibank Canada daily. This information is used to produce an overdraft report over U.S. and Canadian bank accounts, which is used daily within CFS as a tool to identify funding problems and is reviewed weekly with GB's CFO. Matters are investigated where appropriate (Control 11.02).

On a monthly basis, for U.S. bank accounts, CFS receives a report from RISX-FACS® providing aggregate payment information by sub-account. An automated job compares this information to the Issuance Summary report from the bank reconcilement. If the figures match, the bank statement is mailed to the client. Otherwise, investigation is undertaken by CFS and, if necessary, corrective input is performed and contact is made with the client (Control 11.03). For Canadian bank accounts, a manual account reconciliation is performed since the Canadian accounts are stand-alone and no formal out-of-balance report is available. This monthly reconciliation is performed by GB's offshore team. If out of balances are detected, they are investigated and resolved in a timely manner by CFS (Control 11.04).

On a monthly basis, Citibank N.A. places stop pays on issued Citibank U.S. checks with check dates more than 120 days old. This process is called stop-aged. Subsequently, a data file is sent to Gallagher Bassett from Citibank N.A. that is read into RISX-FACS® to update the payment record with stop-aged dates. Errors identified in the processing of the monthly stop-aged load are reviewed by CFS personnel (Control 11.05). A manual process was implemented to manually stop-age checks issued after more than 120 days that are issued from Citibank Canadian bank accounts. GB's offshore team tracks all outstanding Canadian checks. On a monthly basis, all checks identified as outstanding for more than 120 days by the offshore team will be emailed to CFS. Upon notification, CFS fills out a stop payment order form and emails it to Citibank (Control 11.06). After receiving the form, Citibank will stop the payment and send a confirmation back to CFS. Once CFS receives the confirmation, RISX-FACS® will be updated to classify the payment status of the related check to Stop Pay.

EFT

The EFT process is available to all U.S. states; however, certain states do not allow EFT payments, or some clients do not allow certain claimants to receive EFT; therefore, edits were developed to prevent adjusters from requesting an EFT form for those circumstances. If a claimant received services in a specific state or the client does not allow the receipt of EFT funds, RISX-FACS® will not provide the EFT request form. Gallagher Bassett does not perform EFTs for Canadian claimants, clients, or providers.

Adjusters are responsible for offering this option to the claimants. If the claimant is interested, the adjuster submits a request for an authorization form. In order to submit a request, the adjuster selects the EFT Account Maintenance screen from the Payment menu. The adjuster enters the claim number online, and RISX-FACS® populates the name and mailing address information automatically (Control 11.07). The system will not allow more than one EFT account to exist for the same claimant (Control 11.08).

The claimant will complete the authorization form (including a voided check) and mail it to CFS. CFS has the authority to complete the setup process. CFS will review the form for completeness and then set up the access in RISX-FACS®. CFS enters the banking information into RISX-FACS® (account number, routing number, bank information, and effective date).

In addition to providing EFT for claimants, Gallagher Bassett provides EFT setup for providers who have a large volume of payments paid out to them each year. In the past, these payments were paid through the issuance of checks. Once Gallagher Bassett establishes that the provider is willing to be paid through EFT, a provider either fills out a direct deposit authorization form or sends an email to Gallagher Bassett with important information, such as the Tax ID number, a voided check, and other contact information. In addition, at times, Gallagher Bassett obtains the provider's W-9 to verify that the Tax ID number provided on the deposit form is truly their Tax ID number. Gallagher Bassett management calls the provider's bank to verify the accuracy of the information provided. Gallagher Bassett enters the verified EFT information, including the Tax ID number, ABA number, EFT account number, and banking information, on the Provider EFT Maintenance screen in RISX-FACS®. In addition, the system allows only one provider EFT setup per each Tax ID number (Control 11.09). The same provider can have different EFT setups as long as each location has a unique Tax ID number.

Complementary User Entity Controls

In designing its system, the Company has contemplated that certain complementary controls would be implemented by user organizations to achieve certain control objectives included in this report. The complementary user entity controls are listed in "Description of Control Objectives, Controls, Tests, and Results of Tests."

Description of Control Objectives, Controls, Tests, and Results of Tests

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing, and extent of our testing of the controls specified by Gallagher Bassett, we considered the aspects of Gallagher Bassett's control environment and organizational structure, risk assessment process and control activities, information and communication, and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Control Environment and Organizational Structure

- Inquired with IT management and inspected that IT policies included roles and responsibilities.
- Obtained a copy of the code of business conduct and ethics (the Code), inspected the Code for reasonableness of the Code's provisions that address fraudulent and unethical behavior, and determined that employees signed an acknowledgement as to their intent to comply with the Code.
- Inspected IT policies and determined that technology standards were incorporated into overall IT policy.
- Inspected the results of the Conflict of Interest questionnaire completed by Gallagher Bassett employees on an annual basis and inquired with management about the investigation for conflicts identified.
- Inspected evidence that Fraud Detection and Prevention training occurred.

Risk Assessment Process and Control Activities

- Inspected the biennial technology Risk Heat Map assessment and noted that it was updated within the last two years.
- Inspected the risk assessment associated with Gallagher Bassett's claims processing operations.
- Inspected Gallagher Bassett's policies and procedures covering areas such as Policies and Guidelines and Technology Security Standards.

Information and Communication

- Determined that employees are notified of the existence of a fraud hotline on a quarterly basis and independently called the Fraud Hotline to assess its existence.
- Observed at a sample of branch sites that Gallagher Bassett best practices were distributed to branch personnel.

Monitoring

- For a sample of reports, inspected the report reviewed and the tracking spreadsheet maintained by the Operational Security Department and determined that the reports were generated, reviews were occurring appropriately, and issues identified were investigated and resolved as necessary.

No deviations were noted in the testing of entity-level controls.

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of, the Company. The testing performed by Ernst & Young LLP (EY) and the results of tests are the responsibility of the service auditor.

Data and Procedural Controls

Control Objective 1: Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and that deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
1.01	Access to perform scheduling functions is limited to appropriate personnel.	For Netbatch and manual jobs, inspected access rights for users with access to change the job schedule within HP NonStop and, through inquiry with management, determined that access was limited to appropriate personnel.	No deviations noted.
		For Ad Hoc jobs, inspected access rights for users with access to change the job schedule priority of jobs within RISX-FACS® Ad Hoc scheduler and, through inquiry with management, determined that access was limited to appropriate personnel.	One out of a total population of 55 users with Ad Hoc Job Scheduling access had inappropriate access; however, this user did not login to their account during the reporting period. **Management's Response** GB Management is reviewing the procedures for transition of contingent workers to full-time employees. System enhancements have been submitted to verify the termination of the contingent worker ID in this situation This Work Request will be prioritized and developed as resources become available.
1.02	Netbatch jobs are scheduled based on appropriate requests.	For a sample of new jobs, obtained and inspected the Netbatch schedule and determined that jobs were scheduled based on appropriate requests.	No deviations noted.
1.03	Netbatch is configured to notify appropriate personnel upon job failure.	Inspected the Netbatch alert configuration and determined that appropriate personnel were configured to receive an email notification upon job failure.	No deviations noted.
1.04	Errors with major/critical processes are communicated in the Daily Activity Summary Report or carried forward to the shift turnover for continued monitoring and follow-up, if warranted.	For a sample of days, obtained and inspected the Daily Activity Summary Report and determined that errors were communicated and, if warranted, errors were carried forward to the shift turnover for continued monitoring and follow-up.	No deviations noted.

Data and Procedural Controls (continued)

Control Objective 1: Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and that deviations, problems, and errors are identified, tracked, recorded, and resolved in complete, accurate, and timely manner. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
1.05	Daily Activity Reports detailing the jobs to be processed are signed off by the operator indicating time of completion.	For a sample of days, obtained and inspected the Daily Activity Reports and determined that it was updated to indicate whether jobs had been completed and signed off by an operator.	No deviations noted.
1.06	The Schedulers are responsible for scheduling non-routine jobs based on submitted written requests. Non-routine requests are deferred to nonbusiness hours unless approved by management.	For a sample of non-routine jobs processed, obtained and inspected the written request and determined that the jobs were run during nonbusiness hours, unless approved by management.	No deviations noted.
1.07	The Schedule Turnover form is used to track non-routine job requests not completed during the prior shift.	For a sample of days, obtained and inspected the completed turnover form from each shift and determined that each job included a status and was tracked to completion.	No deviations noted.
1.08	Individuals who are responsible for resolving problems are identified in the Disaster Recovery Manual.	Obtained the Disaster Recovery Manual and determined contacts were identified in the manual. Inquired with management and determined that designated Operations management personnel were identified in the Disaster Recovery Manual and would be contacted if problems arose that required management intervention. Inquired with management and determined that no problems occurred during the period that required contact for intervention.	No deviations noted.

Access to Data Files and Programs

Control Objective 2: Controls provide reasonable assurance that physical and logical access to production applications, data, and computer resources is restricted to authorized and appropriate users to (1) protect applications and data from unauthorized modification and (2) support the segregation of duties.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
2.01	Policies and procedures are in place for security administration for RISX-FACS® and HP NonStop (including Guardian and Safeguard).	Obtained policies and procedures and determined they were in place related to: • Granting, changing, and removing access on RISX-FACS® • Granting, changing, and removing access on HP NonStop (including Guardian and Safeguard) • Password protection was in place to restrict access • Periodic review of user access levels	No deviations noted.
2.02	The ability to administer RISX-FACS® security is restricted to appropriate personnel.	For a sample of users with the ability to administer RISX-FACS® security, determined that access was appropriate through inquiry with management and based upon branch managers' periodic review of access.	No deviations noted.
2.03	Access to RISX-FACS® and HP NonStop is granted to internal users based on approved requests.	For a sample of internal users added to RISX-FACS® and HP NonStop, inspected evidence and determined that the level of access granted was based on the approved request.	No deviations noted.
2.04	Client users are set up with read-only access or the ability to add client claim notes.	For a sample of client users added to RISX-FACS®, inspected permissions and determined that only read-only access or the ability to add claim notes was granted.	No deviations noted.
2.05	Terminated employees' access is revoked according to the requested termination date.	For a sample of terminated employees, inspected termination dates and notice dates and determined that the subsequent removal from RISX-FACS® occurred in a timely manner based on the date and time included on the termination request.	For 1 of 25 terminated users sampled, the user's access to RISK-FACS was not removed timely. **Management's Response** GB is modifying RISX-FACS termination processing to synchronize the termination of RISX-FACS application access with Corporate off-boarding notice when application termination notice is not submitted.

Access to Data Files and Programs (continued)

Control Objective 2: Controls provide reasonable assurance that physical and logical access to production applications, data, and computer resources is restricted to authorized and appropriate users to (1) protect applications and data from unauthorized modification and (2) support the segregation of duties. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
2.06	On a quarterly basis, branch management reviews the access to RISX-FACS®. A report is generated for each branch and is sent out to the appropriate persons for review. Changes requested as part of the review are made within the system.	For a sample of quarters, obtained the quarterly review checklist and determined that the review was sent to all branches with RISX-FACS® users. For the sampled quarters, selected a sample of branches and obtained and inspected support for the RISX-FACS® periodic reviews and determined that the review was sent out to the appropriate persons and changes requested as part of the review were made within the system as appropriate.	No deviations noted
2.07	Password settings for RISX-FACS® are set to enforce expiration, length, and complexity. Password settings for HP NonStop are set to enforce expiration (or a policy exception is on file), lockout, length, complexity and history	Obtained and inspected system-generated password settings for RISX-FACS® and determined that the settings in place enforce appropriate expiration, length, and complexity.	No deviations noted.
		Obtained and inspected system-generated password settings for HP NonStop and determined that the settings in place enforce expiration (or a policy exception is on file), lockout, length, complexity and history.	No deviations noted.
2.08	HP NonStop system access log reports are reviewed on a weekly basis by GBIT for inappropriate system configuration changes and forced logon attempts.	For a sample of weeks, obtained and inspected the weekly reports and determined that the report was being generated and reviewed by GBIT.	No deviations noted.

Access to Data Files and Programs (continued)

Control Objective 2: Controls provide reasonable assurance that physical and logical access to production applications, data, and computer resources is restricted to authorized and appropriate users to (1) protect applications and data from unauthorized modification and (2) support the segregation of duties. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
2.09	Privileged HP NonStop IDs are properly restricted.	For all privileged HP NonStop IDs, inquired and determined with management that the IDs were properly restricted.	No deviations noted.
		Inquired with management and determined that a process was in place to grant temporary or emergency access to privileged HP NonStop IDs. Observed that the activity log for privileged HP NonStop IDs (including temporary and emergency accounts) was reviewed daily by management to validate appropriate use.	No deviations noted.
2.10	An adjuster from one branch cannot access the e-Box of an adjuster from another branch.	Obtained a system generated list of users with access to the e-Box for a given branch and validated that users from another branch did not have access.	No deviations noted.
2.11	A quarterly review of the Corporate Data Center access list is performed. Access modifications are implemented as requested.	For a sample of quarters, inspected evidence and determined that access to the primary data center was reviewed for appropriateness and that modifications requested were made.	No deviations noted.
2.12	Firewall system logs are examined weekly with a search utility. Tools are used to monitor network traffic. When a potential service issue is detected, an alert is sent to the LAN/WAN administrator for resolution. Log-on attempts are logged in a security management tool's secure log. The log is monitored at least once a week.	Inquired with management that firewall system logs were examined weekly with a search utility and log-on attempts that were logged were monitored at least once a week for inappropriate access. Obtained management's tracking sheet which includes the review of all weekly logs (firewall system logs and log-on attempts) to date.	No deviations noted.
		Inspected configuration of the network monitoring tools and determined that emails would be sent to LAN/WAN administrators for high/critical alerts.	No deviations noted.

Access to Data Files and Programs (continued)

Control Objective 2: Controls provide reasonable assurance that physical and logical access to production applications, data, and computer resources is restricted to authorized and appropriate users to (1) protect applications and data from unauthorized modification and (2) support the segregation of duties. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
2.13	Access to sensitive system utilities, directories, and scripts used for data transfer is limited to appropriate personnel.	Inspected system access rights and determined that access to sensitive system utilities, directories, and scripts used for data transfer was limited to appropriate personnel.	No deviations noted.

Complementary User Entity Controls

- All clients have access to RISX-FACS.com®. SYS-FACS® clients also have access to classic RISX-FACS®. Clients are responsible for periodically reviewing access levels for client personnel to determine if appropriate.
- Clients are responsible for notifying Gallagher Bassett of terminations/removals of access required for client user access.
- Clients are responsible for notifying Gallagher Bassett of changes in client user access to RISX-FACS® and reviewing the changes for accuracy.

Tape and File Management

Control Objective 3: Controls provide reasonable assurance that data and applications are protected against environmental threats and are backed up to permit restoration of applications and processing in the event of the destruction of the applications or data.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
3.01	Incremental backups are performed on a daily basis, and a full backup is performed on a weekly basis.	For a sample of daily incremental and weekly full backups, inspected documentation and determined that incremental and full backups were performed on a daily and weekly basis, respectively.	No deviations noted.
3.02	Backup and restore management jobs are restricted to appropriate personnel.	Inquired of GTS management and inspected users assigned to back up and restore management jobs and determined that access was restricted to appropriate personnel.	No deviations noted.
3.03	Tapes are rotated based on the retention policy to an off-site location.	For a sample of daily incremental and weekly full backups, inspected documentation and determined that virtual tapes were rotated to an off-site server based on the formal retention policy.	No deviations noted.
3.04	An annual test is performed to determine that data on tapes can be restored and is accurate and complete.	Obtained and inspected documentation and determined that an annual test was performed and that data was successfully restored.	No deviations noted.
3.05	Individuals who are responsible for resolving problems are identified in the Disaster Recovery Manual.	Obtained the Disaster Recovery Manual and determined contacts were identified in the manual. Inquired with management and determined that designated Operations management personnel were identified in the Disaster Recovery Manual and would be contacted if problems arose that required management intervention. Inquired with management and determined that no problems occurred during the period that required contact for intervention.	No deviations noted.

Application Development, Maintenance, and Documentation

Control Objective 4: Controls provide reasonable assurance that application code and configuration parameter changes are initiated as needed, are authorized, and function in accordance with application specifications to (1) result in valid, complete, accurate, and timely processing and data; (2) provide for the functioning of application controls; and (3) support segregation of duties.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
4.01	A formal system development methodology exists and is used in development/maintenance projects to control the design, testing, and implementation of modifications.	Inquired with appropriate personnel and obtained the current system development documentation to validate that a formal system development methodology does exist.	No deviations noted.
4.02	Application program changes, including emergency changes, must be requested. The request must be authorized by the appropriate individual(s) prior to start of development.	For a sample of application program changes, inspected change request forms and determined that the changes were appropriately authorized prior to the start of development.	No deviations noted.
4.03	Development and testing for each application program change is performed in a separate environment than production.	Inspected evidence that separate environments exist.	No deviations noted.
		For a sample of application program changes, inspected evidence and determined that changes went through separate development and test environments.	No deviations noted.
4.04	Testing must be completed and approved for application program changes prior to implementation to production.	For a sample of application program changes, inspected change request forms and determined that changes were tested prior to implementation to production.	No deviations noted.
4.05	Application program changes are approved by appropriate individual(s) prior to migration to production.	For a sample of application program changes, inspected change request forms and determined that changes were approved by appropriate personnel prior to implementation to production.	No deviations noted.
4.06	Developers do not have update access to production, and an individual other than the developer migrates the change into production.	For a sample of application program changes, inspected change request forms and determined that changes were migrated to production by an individual other than the developer.	No deviations noted.
		Inspected evidence that individuals with development responsibilities do not have access to move changes into production, unless authorized.	No deviations noted.

Application Development, Maintenance, and Documentation (continued)

Control Objective 4: Controls provide reasonable assurance that application code and configuration parameter changes are initiated as needed, are authorized, and function in accordance with application specifications to (1) result in valid, complete, accurate, and timely processing and data; (2) provide for the functioning of application controls; and (3) support segregation of duties. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
4.07	Changes to operating systems are authorized, tested, and approved prior to implementation into production.	Inquired with management and determined that changes to operating systems would be authorized, tested, and approved prior to implementation.	No operating system changes were noted during the report period.
4.08	The NonStop security configuration and modifications via Safeguard are appropriately restricted.	For user IDs with the ability to modify Safeguard configurations, inquired with management and determined that the IDs were appropriately restricted and users were authorized.	No deviations noted.

Complementary User Entity Control

- Clients are responsible for being aware of changes affecting the RISX-FACS® applications through periodic communication with Gallagher Bassett Claims Management personnel.

Internet-Related Operations, Monitoring, Maintenance, and Documentation

Control Objective 5: Controls provide reasonable assurance that network infrastructure is configured as authorized to (1) enable applications and application controls to operate effectively, (2) protect data from unauthorized changes to provide for its availability for processing, and (3) support segregation of duties.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
5.01	Gallagher Bassett uses SSL when transferring information between the user, the Gallagher Bassett server, and server to server.	Inspected settings and the certificate information and determined that SSL was current and active.	No deviations noted.
5.02	Changes to the web servers, firewall, and routers are tracked and approved through the Change Management database in Remedy.	For a sample of changes, inspected the Remedy change form and determined that the change was appropriately approved.	No deviations noted.
5.03	Firewall system logs are examined weekly with a search utility. Tools are used to monitor network traffic. When a potential service issue is detected, an alert is sent to the LAN/WAN administrator for resolution. Log-on attempts are logged in a security management tool's secure log. The log is monitored at least once a week.	Inquired with management that firewall system logs were examined weekly with a search utility and log-on attempts that were logged in a secure log were monitored at least once a week for inappropriate access. Obtained management's tracking sheet which includes the review of all weekly logs (firewall system logs and log-on attempts) to date.	No deviations noted.
		Inspected configuration of the network monitoring tools and determined that emails would be sent to LAN/WAN administrators for high/critical alerts.	No deviations noted.
5.04	Web server configurations are in place and are set up in accordance with Gallagher Bassett standards.	Inquired with the system administrator about the web server configurations. Inspected the configurations and determined that they were in place and set up in accordance with Gallagher Bassett standards.	7 Windows services on RISX-FACS® servers do not conform to Corporate Server Policy. **Management's Response** The services that do not conform to Corporate Server Policy are non-critical and low-critical services and have a low surface for exploit. These services were turned off by 1 June 2013. Servers are now built and going forward will be built per AJG Corporate Policies.
5.05	Access to sensitive system utilities, directories, and scripts used for data transfer is limited to appropriate personnel.	Inspected system access rights and determined that access to sensitive system utilities, directories, and scripts used for data transfer was limited to appropriate personnel.	No deviations noted.

Claims Processing

Control Objective 6: Controls provide reasonable assurance that losses, claims, reserves, and related adjustments are authorized, accurate, and processed in accordance with Gallagher Bassett guidelines and client service instructions.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
6.01	New claims are entered within RISX-FACS® based on the initial notice of the loss.	For a sample of branches, selected a sample of claims set up during the reporting period and inspected the accident report and the claim within RISX-FACS® to determine that the file was set up accurately.	No deviations noted.
6.02	RISX-FACS® automatically checks for duplicate claims and provides the adjuster with a listing of possible duplicates.	Observed that the system automatically checks for duplicate claims and provides the adjuster with a listing of possible duplicates based on set criteria.	No deviations noted.
6.03	A claim setup review is performed by the supervisor on all claims types, except medical only.	For a sample of branches, selected a sample of claims (excluding medical only claims) open for at least 30 days during the reporting period and inspected claim setup reviews to determine that they were performed by the claim supervisor and that the claim note appeared valid and appropriately addressed the claim.	For 2 of 42 claims sampled, the claim setup review was not performed by the claim supervisor. **Management's Response** Branch Managers have access to supervisor's diaries to determine if there are any reviews that are past due. Branch Managers are responsible for following up with each supervisor for timely completion. We have re-communicated to these offices, and the field overall, the requirements for completing supervisory reviews in a timely manner.
6.04	Initial reserves are established at the time of claim set up.	Observed that the system does not allow a claim to be set up without the adjuster setting a reserve.	No deviations noted.

Claims Processing (continued)

Control Objective 6: Controls provide reasonable assurance that losses, claims, reserves, and related adjustments are authorized, accurate, and processed in accordance with Gallagher Bassett guidelines and client service instructions. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
6.05	Initial contact with the appropriate party/parties is completed within the appropriate time frame after receipt of the claim.	For a sample of branches, selected a sample of claims and determined that contact was made appropriately.	For 1 of 40 claims sampled, the initial contact was not made timely after the receipt of the claim. **Management's Response** This policy was reviewed and discussed with Zone and Branch management. Contact compliance is monitored by Branch Management and Zone Management. This instance was 12 hours beyond our requirements on this minor property damage claim. The appropriate time frame for this type of claim is to make contact within 24 hours.

Claims Processing (continued)

Control Objective 6: Controls provide reasonable assurance that losses, claims, reserves, and related adjustments are authorized, accurate, and processed in accordance with Gallagher Bassett guidelines and client service instructions. (continued)

	Controls Specified by the Company	Testing Performed by EY	Results of Testing
6.06	Subsequent supervisory reviews are performed on a timely basis after the initial claim setup review, unless otherwise stated in the client service instructions, to help ensure reserves are appropriate based on facts known to date. A review is considered to be timely if it is performed within 100 days after the initial claim setup review. Claims not in compliance with their supervisory review schedule are brought to branch management's attention, and a supervisory review is performed.	For a sample of branches, selected a sample of claims open for at least 130 days during the reporting period and inspected subsequent supervisory reviews to determine that they occurred within 100 days of the claim setup review, unless otherwise stated in the client service instructions, and observed that a note was entered in the system addressing the appropriateness of reserve estimates based on facts known to date.	For 1 out of 40 claims sampled, the subsequent supervisory review was completed but not performed timely. **Management's Response** Branch Managers have access to supervisor's diaries to determine if there are any reviews that are past due. Branch Managers are responsible for following up with each supervisor for timely compliance. We have re-communicated to the Branch Managers the requirements for completing supervisory reviews timely and the importance of utilizing the diary escalation process. In addition, there is a monthly corporate roll-up process that is distributed to each zone and branch, showing their compliance with the subsequent supervisory reviews. The Vice Presidents within each zone are responsible for following up with the Branch Managers to discuss compliance, as necessary. Gallagher Bassett averaged approximately 93% of claims in compliance with the subsequent supervisory reviews across all U.S. and Canadian branches.
		Inspected aggregate compliance numbers for all U.S. and Canadian branches for the reporting period and validated that, on average, more than 90% of all claims across these branches were in compliance with the supervisory review schedule.	No deviations noted.

Claims Processing (continued)

Control Objective 6: Controls provide reasonable assurance that losses, claims, reserves, and related adjustments are authorized, accurate, and processed in accordance with Gallagher Bassett guidelines and client service instructions. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
6.07	Authorization is obtained from the client for reserve changes exceeding thresholds established in the client service instructions.	For a sample of branches, selected a sample of clients and identified the reserve authorization thresholds specified within their client service instructions, selected a sample of reserve changes meeting those thresholds, and determined through inspection of claim notes in RISX-FACS® that reserve changes were communicated to the client and authorization was obtained.	For 3 of 40 reserve changes, client authorization was not obtained. These 3 reserve changes were for 1 of the 10 clients sampled. Subsequently, an additional 25 reserve changes, across 7 additional clients, were sampled and no further deviations were noted. **Management's Response** The 3 above noted deviations did occur with one adjuster, on one account. The adjuster has a monthly open file review with the account where status is discussed on each open file. In these 3 instances, the adjuster failed to obtain the authorization in writing and document in claim notebook. The client was contacted upon discovery of the findings and provided a written approval which was subsequently documented in claim notebook. Reserving protocol has been reviewed with the Branch Management Staff, as well as the handling adjuster, reminding the staff that reserve increases requiring client approval must be obtained in writing and documented in claim notebook prior to making the actual change. No additional deviations noted on the remainder of the sample.

Claims Processing (continued)

Control Objective 6: Controls provide reasonable assurance that losses, claims, reserves, and related adjustments are authorized, accurate, and processed in accordance with Gallagher Bassett guidelines and client service instructions. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
6.08	RISX-FACS® will not allow an adjustment of reserves reaching a total experience of $5,000 for a workers' compensation claim without the adjuster completing a Total Experience Worksheet, which is a detailed breakdown of the reserves.	Observed that the system does not allow an adjustment of reserves reaching a total experience of $5,000 or greater for a workers' compensation claim without the adjuster completing a Total Experience Worksheet.	No deviations noted.
6.09	On a monthly basis, a Controlled Loss Warning Report is sent to the GB Service Center for claims that reach severity, dollar, or timing triggers. The actions taken for each claim are documented in the monthly report.	For a sample of branches, selected a sample of months and inspected the Controlled Loss Warning Reports to determine that proper notification occurred and actions taken for each warning were documented in the monthly report.	No deviations noted.

Complementary User Entity Controls

- Clients are responsible for periodically reviewing the RISX-FACS® Claim Register and the RISX-FACS® Claim Activity Report for reasonableness, timeliness, and validity of claims activity.
- Clients are responsible for periodically reviewing the RISX-FACS® Payment and Recovery Register and the RISX-FACS® Specific Excess Report for reasonableness and timeliness.
- Clients are responsible for periodically reviewing the client service instructions to determine that these are in accordance with the established client service contract.
- Clients are responsible for periodically reviewing the client service contracts with Gallagher Bassett and the RISX-FACS® Payment and Recovery Register Report for compliance with payment authorization levels and timeliness.

Payment Processing

Control Objective 7: Controls provide reasonable assurance that claims payments and related adjustments are authorized, accurate, processed, and issued to legitimate payees in accordance with Gallagher Bassett guidelines and client service contracts.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
7.01	Claims payments in excess of $50,000 or the amount specified in client service contracts must be approved by the payment authorizer, unless specified differently in the client service contracts.	For a sample of branches, selected a sample of claims payments made over $50,000 or the amount specified in the client service contracts and inspected payment authorization reports to determine that the payments were appropriately approved.	No deviations noted.
7.02	RISX-FACS® will place payments exceeding the authorization limit in a Hold status and require approval by the payment authorizer to release payment.	Observed branch personnel attempt to submit a payment over the authorization limit and determined that RISX-FACS® placed the payment in a Hold status awaiting subsequent approval in order to release the payment.	No deviations noted.
7.03	RISX-FACS® requires the payment breakdown to equal the payment amount as a validity check. If the sum of the payment breakdown and the payment amount entered are not identical, RISX-FACS® will not allow the payment to be entered into the system.	Observed branch personnel attempt to submit a payment where the sum of the payment breakdown did not equal the payment amount and determined that RISX-FACS® did not allow payment.	No deviations noted.
7.04	RISX-FACS® prevents the processor from requesting a payment in excess of the remaining reserve.	Observed branch personnel attempt to enter a payment in excess of the remaining reserve and determined that RISX-FACS® displayed an error message.	No deviations noted.
7.05	Reconciliation of check control totals between the check-printing service and Gallagher Bassett is performed on a daily basis. Issues identified are investigated and resolved.	For a sample of days, inspected the Banking Activity Sheets and determined that a reconciliation was performed and, if applicable, issues were investigated and resolved.	For 1 of 25 days sampled, evidence of the reconciliation was not retained. Subsequently, an additional 15 days were sampled and no further deviations were noted. **Management's Response** This issue was caused during the transitioning of the reconciliation process from a manual form to an electronic form. The issue will not be repeated as it is now in electronic form and all on the shift have access to the form, not one supervisor as was per the previous process. The electronic form is covered with the Turnover Manager as part of the shift turnover.

Payment Processing (continued)

Control Objective 7: Controls provide reasonable assurance that claims payments and related adjustments are authorized, accurate, processed, and issued to legitimate payees in accordance with Gallagher Bassett guidelines and client service contracts.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
7.06	Reconciliation of EFT control totals between the banking service and Gallagher Bassett is performed on a daily basis. Issues identified are investigated and resolved.	For a sample of days, inspected the Banking Activity Sheets and determined that the EFT reconciliation was performed and, if applicable, issues were investigated and resolved.	No deviations noted.
7.07	The supervisor reviews the Banking Reconciliation Packet to validate that all steps were completed.	For a sample of days, inspected the Daily First Shift Balancing Checklist and determined that the supervisor validated that all steps were completed, as notated by the initials on the packet.	No deviations noted.
7.08	RISX-FACS® automatically checks for duplicate payments and provides the adjuster with a listing of possible duplicates.	Observed that RISX-FACS® automatically showed a listing of possible duplicates to an adjuster when attempting to submit a payment.	No deviations noted.
7.09	e-Bill and e-Invoice claim payments are substantiated by vendor bill image for e-Bill and by claim documentation for e-Invoice.	For a sample of branches, selected a sample of payments made on e-Bills and e-Invoices and inspected vendor bill images or claim documentation used by the claims representatives to determine that the e-Bills and e-Invoices were processed appropriately.	No deviations noted.
7.10	A review is performed by the GBSC on a daily basis to investigate and resolve instances where the secondary authorizer is the adjuster or the issuer for payments over $50,000.	For a sample of days, inspected the Fraud Detection Review report and the Branch Referral Tracking spreadsheet maintained by the Operational Security Department and determined that the authorization review was occurring appropriately, and any issues identified were investigated and resolved as necessary.	No deviations noted.

Payment Processing (continued)

Control Objective 7: Controls provide reasonable assurance that claims payments and related adjustments are authorized, accurate, processed, and issued to legitimate payees in accordance with Gallagher Bassett guidelines and client service contracts. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
7.11	Stop-pay transmissions on U.S. bank accounts are fed into RISX-FACS® daily from Citibank N.A. and are matched to issued checks. The checks that are matched to the transmission are marked as stop paid in RISX-FACS®. For checks issued by the Canadian branch, CFS submits a stop-pay request for the bank. Upon confirmation from the bank that the stop-pay hold was placed, CFS changes that status of the check in RISX-FACS® to stop paid.	Inquired and determined with management that checks coded as stop paid in RISX-FACS® originated from a Citibank N.A. file, which was transmitted into RISX-FACS® through a nightly job.	No deviations noted.
		For an example stop pay check, inspected RISX-FACS® and determined that the issued check with the same amount and check number was stopped on the correct date.	No deviations noted.
		For Citibank Canadian bank accounts, selected a sample of stop-pay checks and determined that the RISX-FACS® status was updated to reflect a stop-pay status.	No deviations noted.
7.12	Reports are generated and examined for suspicious activity that may have resulted in payments being issued to inappropriate payees. Issues identified are investigated and resolved.	For a sample of daily reports, inspected the Fraud Detection Review report and the Branch Referral Tracking spreadsheet maintained by the Operational Security Department and determined that the reports were generated, reviews were occurring appropriately, and issues identified were investigated and resolved as necessary.	No deviations noted.
7.13	The system searches for possible duplicate e-Bills based on a certain set of criteria. On a monthly basis, a report is sent to each vendor identifying the possible duplicates.	For a sample of months, selected a sample vendor and inspected reports sent to the vendor and noted that a list of possible duplicates was identified and appropriately communicated to the vendor.	No deviations noted.

Payment Processing (continued)

Control Objective 8: Controls provide reasonable assurance that physical access over checks and field pay documentation is limited to authorized personnel.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
8.01	Manual checks are maintained in a folder located in a locked cabinet. Only select individuals have the keys to this cabinet.	For a sample of branches, inspected the manual check folder and determined that checks on-hand at the branches correlate with the check inventory maintained by the corporate home office and that all checks were accounted for.	No deviations noted.
		Inspected the location where manual checks are stored at a sample of branches and noted that they were stored in locked cabinets with restricted access. Discussed with branch management and determined that only select individuals had keys to the cabinets and that access was appropriate.	No deviations noted.
8.02	Requests for manual checks are recorded and tracked in a log.	For a sample of branches, selected a sample of completed field payments and inspected the log to determine that checks were noted within the log.	No deviations noted.
8.03	At the end of each month, the reconciler reviews the log to ascertain that unused checks are in the folder and checks that have been issued for that month are included in the log. The log is signed off, indicating the completion of the review.	For a sample of branches, selected a sample of months and inspected the manual check logs to determine that a review was performed as notated by the signature on the log.	No deviations noted.
8.04	Authorized personnel must sign the manual check for issuance to the payee.	For a sample of branches, selected a sample of completed field payments and inspected the copied check retained at the branch location or at the corporate office to determine that the appropriate authorizer signed the check.	No deviations noted.
8.05	The original check can be handled by only the designated check handler at the branch.	For a sample of branches, inquired and observed with branch management that the original check could be handled by only the designated check handler.	No deviations noted.

Complementary User Entity Control

- Clients are responsible for periodically reviewing the RISX-FACS® Payment and Recovery Register and the RISX-FACS® Specific Excess Report for reasonableness and timeliness.

Recoveries Processing

Control Objective 9: Controls provide reasonable assurance that claims recoveries are accurately and completely processed.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
9.01	Authorized home office personnel apply recoveries and update the claim payment status in RISX-FACS®.	For a sample of branches, selected a sample of recoveries and inspected recovery detail to determine that authorized corporate home office personnel applied the recovery.	No deviations noted.
9.02	Recoveries for clients with Citibank accounts are directly deposited into their bank accounts. Other recovery checks are endorsed and mailed to the appropriate party.	For a sample of branches, selected a sample of recoveries and determined that deposits of recoveries to Citibank accounts and mailing of recoveries for non-Citibank accounts occurred through inspection of Citibank bank statement/deposit notices.	No deviations noted.
9.03	Recovery of funds is entered into RISX-FACS® by branch personnel based on the information included on the recovery check or automatically processed and programmatically entered into RISX-FACS® for some managed care vendors.	For a sample of branches, selected a sample of recoveries and inspected claim files to determine that the recovery information in RISX-FACS® matched the information on the recovery check for manually processed recoveries or in the data file provided by the managed care vendor for automatically processed recoveries.	No deviations noted.
9.04	Excess recoveries are initiated and entered into RISX-FACS® based on calculations derived from recovery checks or other supporting documentation.	For a sample of branches, selected a sample of excess recoveries and inspected excess recovery documentation to determine that the initiated recovery matched the information in RISX-FACS®.	No deviations noted.

Client Reporting

Control Objective 10: Controls provide reasonable assurance that data output and documents from RISX-FACS® are distributed accurately to clients on a timely basis.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
10.01	For clients that elect to receive client reports, the reports are transmitted per client-designated frequency via email, RISX-FACS®, CD-ROM, and/or paper.	For a sample of new clients, inspected the setup instructions that indicate the client-requested frequency and media method used to transmit reports. Compared the report frequency and media method in RISX-FACS® to that requested in the setup instructions and determined that reports were transmitted as requested or according to the default if no special setup was requested.	No deviations noted.
10.02	Special reports (reports outside the standard set) and changes in frequency and media (to standard or special reports) are set up by IDS in the system based on client requests.	For a sample of new clients, inspected the Notice of Sale and the RISX-FACS® distribution screen and determined that the transmittal of special reports and changes in frequency and media were appropriately set up within the system.	No deviations noted.
10.03	Automated system checks comparing previous month totals plus current period activity validate that reports are in balance. Automated system checks generate automatic escalations for out-of-balance reports.	Obtained and inspected the system checks and determined that they compared previous month totals plus current period activities to help ensure that reports are in balance. Determined that out-of-balance reports generated an automated escalation.	No deviations noted.
10.04	Automated system checks validate that report distribution processes are completed in a timely manner without error.	For a sample of new clients, inspected the report status screen within RISX-FACS® and determined that reports were being created and distributed accurately and successfully and in a timely manner. If any errors occurred in processing, reviewed the follow-up completed to resolve the errors.	No deviations noted.
10.05	For paper-provided reports, a reconciliation between Gallagher Bassett and the report printing vendor service is performed on a monthly basis to determine that the reports are distributed appropriately to recipients.	For a sample of months, inspected the reconciliations performed and determined that reconciling differences, if any, were resolved.	No deviations noted.

Complementary User Entity Control

- Clients are responsible for periodically reviewing the standard reports generated from the RISX-FACS® system, as well as any other special reports, and determining if these are in accordance with the client service contract.

Cash Management

Control Objective 11: Controls provide reasonable assurance that cash accounts are properly set up and maintained.

Controls Specified by the Company		Testing Performed by EY	Results of Testing
11.01	For SIMMS clients, Banking Parameter Agreements designate the method to be used to fund the bank account.	For a sample of new SIMMS setups, inspected the Banking Parameter Agreements and determined that banking was set up in RISX-FACS® appropriately. Determined that the request sent to the bank included the same banking information.	No deviations noted.
11.02	Client Financial Services management examines an overdraft report on a periodic basis and investigates matters where appropriate.	For a sample of weeks, determined that Client Financial Services management examined the overdraft report for U.S. and Canadian bank accounts and investigated matters where appropriate.	No deviations noted.
11.03	On a monthly basis, a system-generated report reconciles aggregate payment information by sub-account between RISX-FACS® and Citibank for U.S. bank accounts. For any items out of balance, investigation is undertaken by Client Financial Services and, if necessary, corrective input is performed and contact is made with the client.	For a sample of months, inspected the completeness and accuracy of the system-generated reconcilement process. In addition, for a sample of months, inspected evidence for a sample of out-of-balance items and determined that actions were taken as dictated by the results of the reconciliation.	No deviations noted.
11.04	For Canadian bank accounts, a manual account reconciliation is performed on a monthly basis. If out of balances are detected, they are investigated and resolved in a timely manner.	For a sample of months, obtained evidence of the manual account reconciliation performed and determined that out of balances, if any, were resolved in a timely manner.	For 1 of 2 months sampled, 1 of 12 account reconciliations tested was not completed timely. **Management's Response** The CFS Manager has reviewed the current process with the service center responsible for these reconciliations. Biweekly meetings have been implemented to monitor the service center's progress. A monthly review and sign-off will be performed by the CFS Manager to help ensure that work is completed timely and variances are investigated and resolved.

Cash Management (continued)

Control Objective 11: Controls provide reasonable assurance that cash accounts are properly set up and maintained. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
11.05	A monthly transmission listing checks that have been stop-aged for being outstanding for more than 120 days is received from Citibank for U.S. bank accounts and loaded into RISX-FACS® where the checks are coded to be listed as stop-aged. Discrepancies in the monthly stop-aged load are identified in a rejects report, which Client Financial Services investigates and resolves each month.	For a sample of months, inspected the monthly stop-aged job schedule and job completion status and determined that the job was completed successfully. For an example stop-aged check, inspected system evidence and determined that the stop-aged check loaded into RISX-FACS® matched the stop-aged check received from Citibank N.A.	No deviations noted.
		Inquired and observed with Operations and Client Financial Services personnel the process in place to investigate rejects. For a sample of months, inspected evidence of the rejects and determined that investigation was performed, where applicable.	No deviations noted.
11.06	On a monthly basis, a reconciliation is performed between RISX-FACS® and Citibank Canadian accounts to identify any checks outstanding over 120 days. Identified checks will be communicated to Citibank and stopped. Upon confirmation from Citibank, checks will be updated in RISX-FACS as stop-aged.	For a sample of months, obtained evidence of the manual account reconciliation performed and determined that outstanding checks over 120 days identified as not stopped at Citibank, if any, were communicated to Citibank, stopped, and the status updated to stop-aged in RISX-FACS®.	No deviations noted.
11.07	EFT application forms are submitted for EFT setup. Setup in RISX-FACS® is based on the information included on the EFT application form or email.	For a sample of new EFT setups, inspected the EFT application forms and/or emails and determined that the EFT was set up in RISX-FACS® accurately.	No deviations noted.
11.08	RISX-FACS® will not allow more than one EFT account to exist for the same claimant.	Observed branch personnel attempt to create an EFT account for a claimant with an existing EFT account and determined that RISX-FACS® displayed an error message.	No deviations noted.

Cash Management (continued)

Control Objective 11: Controls provide reasonable assurance that cash accounts are properly set up and maintained. (continued)

Controls Specified by the Company		Testing Performed by EY	Results of Testing
11.09	RISX-FACS® will not allow more than one EFT account to exist for the same provider Tax ID number.	Observed home office personnel attempt to create an EFT account for a provider Tax ID number with an existing EFT account and determined that RISX-FACS® would not allow another EFT account to be established for that same Tax ID number.	No deviations noted.

Complementary User Entity Controls

- Clients are responsible for reviewing the monthly Citibank bank reconcilement reports for reasonableness.
- Clients are responsible for handling and controlling the issuance of payments if they utilize voucher banking.

Other Information Provided by Gallagher Bassett Services, Inc.

This section is intended to provide interested parties with other information about Gallagher Bassett.

Disaster Recovery Planning

A formal Disaster Recovery Manual is maintained by GBIT for both the HP NonStop and client server environments. The manual is the basis for the disaster recovery plan and is updated when conditions change within the data center that relate to disaster recovery. The Disaster Recovery Manual covers aspects such as:

- GBIT and AJG Shared Services teams involved during a disaster
- GBIT and AJG Shared Services contacts for various duties and components
- Network configuration
- System down/degraded guidelines and responsibilities
- Storage requirements for backup tapes
- Tape storage label numbers
- Vendor information
- Hardware components
- Steps for bringing up the system

Separate lists are maintained covering all SYS-FACS® clients, disaster recovery steps, what constitutes a disaster, and who to initially contact.

Gallagher Bassett Services maintains a backup "warm site" in the Itasca, Illinois office. Corporate home office operations are moved to this site if a disaster should occur. The backup/restore portion of the plan was tested in October 2012.

In a disaster, GBIT and AJG Shared Services are responsible for moving operations to the warm site, recovering the systems, and establishing the communications facilities.

Verizon and SAVVIS Data Centers

The Primary Data Center, located at the SAVVIS Data Center in Elk Grove, Illinois (Verizon facility in Manassas, Virginia prior to November 2012), provides UPS power to the equipment at the facility, including the HP NonStop platform. It should also be noted that the HP NonStop platform is built to withstand any surges and brief disruptions of 30 minutes or less but not a full power outage extending beyond 30 minutes. If the power or voltage goes below a specified level, the HP NonStop platform will contact the HP NonStop Support Center to notify them of the power situation. In turn, the Support Center will call GBIT personnel. In addition, the HP NonStop platform is built with mirrored hard drives. Thus, if one hard drive fails, the other drive will post appropriate alerts and continue processing as if no failure occurred.