VERISK ANALYTICS, INC.

ClaimSearch® Platform

SOC 3

System and Organization Controls (SOC) for Service Organizations Report for the period of January 1, 2022 to December 31, 2022

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

We have examined Verisk Analytics, Inc.'s (the "Company" or "Verisk") accompanying assertion titled *Verisk Analytics, Inc.'s Assertion* (the "Assertion") indicating that the controls within the ClaimSearch® Platform (the "System') were effective for the period of January 1, 2022 to December 31, 2022 (the "Specified Period"), to provide reasonable assurance that Verisk Analytics, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses CyrusOne, a subservice organization, for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. In addition, the Company uses Amazon Web Services (AWS), a subservice organization, for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses various AWS Platform-as-a-Service components such as Amazon Relational Database Services (RDS) and AWS Simple Storage Service (S3). Certain AICPA Applicable Trust Services Criteria specified in the section titled Verisk Analytics, Inc.'s Description of the Boundaries of its System, under the section Subservice Organizations, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. The Assertion does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled *Verisk Analytics, Inc.'s Description of the Boundaries of its System*, under the section *User Entity Controls*, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Verisk Analytics, Inc.'s Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the Applicable Trust Services Criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that the controls within the system were throughout the period to provide reasonable assurance that the service organizatin’s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements;
- Assessing the risks that the controls were not effective to achieve the Company’s service commitments and system requirements based on the Applicable Trust Services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company’s service commitments and system requirements based on the Applicable Trust Services Criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other matters

We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *Verisk Analytics Inc.’s Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, Verisk Analytics, Inc.’s assertion that the controls within the Company’s System were effective throughout the Specified Period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the Applicable Trust Services Criteria, in all material respects, is fairly stated.

Aprio, LLP

Aprio, LLP

Atlanta, Georgia
February 3, 2023

II. Verisk Analytics, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over Verisk Analytics, Inc.'s (the "Company" or "Verisk") ClaimSearch® Platform (the "System") for the period of January 1, 2022 to December 31, 2022 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy (the "Applicable Trust Services Criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). The Company's objectives for the system in applying the Applicable Trust Services Criteria are embodied in its service commitments and system requirements relevant to the Applicable Trust Services Criteria. The principal service commitments and system requirements related to the Applicable Trust Services Criteria are specified in the section titled *Verisk Analytics, Inc.'s Description of the Boundaries of its System*.

The Company uses CyrusOne, a subservice organization, for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. In addition, the Company uses Amazon Web Services (AWS), a subservice organization, for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses various AWS Platform-as-a-Service components such as Amazon Relational Database Services (RDS) and AWS Simple Storage Service (S3). Certain AICPA Applicable Trust Services Criteria specified in the section titled *Verisk Analytics, Inc.'s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *Verisk Analytics, Inc.'s Description of the Boundaries of its System*, under the section *User Entity Controls* can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by User Entities.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.

III. Verisk Analytics, Inc.'s Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Verisk Analytics, Inc. (the "Company" or "Verisk") as it relates to its ClaimSearch® Platform (the "System") for the period of January 1, 2022 to December 31, 2022 (the "Specified Period"), for the trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

Verisk Corporate Overview

Verisk provides predictive analytics and decision support solutions to customers in:

- Insurance
- Energy and specialized markets
- Financial services

Using advanced technologies to collect and analyze billions of records, Verisk draws on unique data assets and deep domain expertise to provide first-to-market innovations that are integrated into customer workflows.

Verisk's Analytics' solutions address insurance underwriting and claims, fraud, regulatory compliance, natural resources, catastrophes, economic forecasting, geopolitical risks, as well as environmental, social, and governance (ESG) matters.

Verisk helps customers make better decisions about risk, investments, and operations with greater precision, efficiency, and discipline. In the United States and around the world, Verisk helps customers protect people, property, and financial assets. Verisk creates exceptional value for its stakeholders through its four distinctives that guide the Company:

Unique Data Assets

Verisk uses its proprietary data assets to develop predictive analytics and transformative models for their customers. Verisk discovers insightful ways to use data, visualize it, and make it meaningful for decisions. Verisk creates innovative solutions by applying scientific methods to massive volumes of data – information about properties and communities, fraud, claims, catastrophes and weather, consumer behavior, insurance premiums and losses, societal and environmental risks, and natural resources.

Deep Domain Expertise

Verisk has specialized and in-depth knowledge in many defined vertical markets, including insurance, energy and natural resources, financial services, environmental health and safety, and government and industry. Verisk understands that different verticals require different approaches, and its deep domain expertise adds value to the analytics in the markets it serves.

Steady Stream of First-to-Market Innovations

Innovation is vital to growth and achieving success. Verisk is on a continuous quest to be the first to market with new innovations. Verisk achieves that by forming strong relationships with its customers as development partners. Innovation takes concerted effort and great motivation. It takes talent, forward thinking, and passion. But the rewards are great – for Verisk, its customers, and shareholders.

Deep Integration into Customer Workflows

By integrating its products and services into customer workflows, Verisk helps its customers better understand and manage risk and make smarter decisions. Through ongoing collaboration, Verisk combines its data, analytics, and decision support platforms into comprehensive, industry-leading solutions.

Verisk VIT Managed Services

The scope of this report is the services as described below that are provided by Verisk Information Systems & Technology Managed Services to various Verisk business units.

Services Provided

Verisk's Managed Services provides infrastructure engineering, operations, service delivery, physical, environmental, and networking services as listed below. Verisk's business units that receive each of these services are considered to be part of "Managed Services", while those businesses receiving just physical, environmental, and networking services are considered to be part of the "Colocation Services" option. Enterprise Risk Management (ERM) delivers critical risk management services across Verisk's enterprise, including Global Security Services (data and cyber security), Information Risk Management, Compliance, Privacy, and Physical Security.

Services	Managed Services		Colocation Services
	On-Premises	Cloud Operations	
Physical and Environmental	X		X
Backup and Restore	X		Optional
"Defense-in-Depth" Protection	X	X	Optional
Incident Management	X	X	Optional
Dedicated Service Desk Support	X	X	Optional
Secure Configuration and Software Distribution	X	X	Optional
Business Continuity Planning and Disaster Recovery	X		Optional
Data Quality Standards and Practices	X	X	Optional
Global Security and Privacy Practices	X	X	Optional

Enterprise Services

There are certain Managed Services, such as onboarding, off boarding, security and incident monitoring, and risk management, which are provided at a Verisk Analytics entity or enterprise level for various business units throughout Verisk. The Verisk business units receiving some or all of these Managed Services during all or some of the period represented by this report include:

- Verisk 3D Visual Intelligence
- Claims Solutions / Fraud Analytics
- Property Estimating Solutions
- Verisk Maplecroft
- Wood Mackenzie

- Underwriting Solutions
- Flexible Architecture and Simplified Technology Hosting Services (FAST)
- Insurance Information Exchange (iiX)
- Nautilus Platform
- Specialty Business Solutions Managed Services
- Whitespace Platform
- Extreme Events Solutions
- ClaimSearch® Platform

Colocation Services

There are certain Colocation Services or data center services, such as physical security, environmental safeguards, networking services, and backup services, which are provided by Verisk Managed Services for business units throughout Verisk. The Verisk business units receiving some or all of these Colocation Services during all or some of the period represented by this report include:

- Insurance Information Exchange (iiX)
- ClaimSearch® Platform
- Extreme Events Solutions
- Verisk Financial Services
- Atmospheric and Environmental Research (AER)

These services are carried out in Verisk's Data Centers as well as in hosted environments managed by Verisk's Cloud Operations team. Managed Services do not extend to services, products, or reports produced by any other operating units of Verisk.

ClaimSearch® Platform

ClaimSearch® is a unit of ISO Services, Inc., a member of the Verisk Analytics (Nasdaq: VRSK) family of businesses. Each year, participating organizations submit tens of millions of reports on individual insurance claims. ClaimSearch's main operations are located at Verisk headquarters in Jersey City, New Jersey. During the scope of this report, ClaimSearch® used Verisk's Eastern and Western Data Centers located in New Jersey and Utah and is now fully migrated to Amazon Web Services (AWS), for the storage and processing of client data.

Through ClaimSearch®, participating organizations can access a variety of services for claims adjudication, investigation, and fraud purposes. Participating organizations electronically submit hundreds of thousands of claims per day in all lines of business, including property, casualty, and automobile insurance. ClaimSearch® automatically loads these claims into the database; then the system searches to find other claims filed by the same individual or business, either as a claimant or as an insured. The database plays an integral role in the fight against insurance fraud and automobile theft.

Participating Organizations that access the data contained within ClaimSearch® use the data in ways consistent with the privacy obligations and any other terms and provisions of the Gramm-Leach-Bliley Act (15 U.S.C., Section 6801 et seq) and any similar state or local statutes, rules, and regulations; the Federal Drivers Privacy Protection Act (18 U.S.C., Section 2721 et seq); the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HIPAA privacy regulations 45 C.F.R. Part 164, the HIPAA security regulations 45 C.F.R. Part 16X, the Health Information Technology for Economic and Clinical Health (HITECH) Act Pub. L. No. 111-005, the Final HIPAA Omnibus Rule, and any similar state and local statutes, rules, and regulations; and such legislation, rules, and regulations as may be enacted by any federal, state, or local government body.

In addition, Participating Organizations shall not use any information they receive from ClaimSearch® for consumer credit purposes, consumer insurance underwriting, employment purposes, or any other purpose covered by the federal Fair Credit Reporting Act (15 U.S.C., Section 1681 et seq) or similar state or local statutes, rules, or regulations.

ClaimSearch® participating organizations are the National Insurance Crime Bureau (NICB) and those organizations credentialed by ClaimSearch® to obtain access to ClaimSearch®. Participating organizations can include, but are not limited to, insurers; third-party administrators; self-insured organizations; pool administrative trusts; automobile rental, auction, and finance organizations; state workers' compensation funds; and claim service providers. Verisk maintains the right, at its sole discretion, to authorize access to ClaimSearch® in the best interest of the participating organizations. NICB participating organizations are those organizations credentialed by the NICB for access to ClaimSearch®. These organizations can include, but are not limited to, law enforcement, criminal justice, and regulatory agencies.

C. System Overview

Services offered by ClaimSearch® are either hosted within the production environment at the Verisk Eastern Data Center or a private cloud-based environment via Amazon Web Services ("AWS").

Data Center Services (Colocation Services provided by Verisk Managed Services)

1. Infrastructure

The Eastern Data Center (EDC) is located in New Jersey, while the Western Data Center (WDC) is located in Utah. The primary International Data Center is located in England, with a backup site located in Germany. Only the WDC is included in the scope of this report as it relates to environmental controls. The Eastern and International Data Center locations' physical and environmental controls are the responsibility of a third-party subservice organization, and therefore, those locations are not in scope for this report. For additional details about the subservice organization's responsibilities, please see the section H: *Subservice Organizations.*

Verisk's Data Centers have numerous information systems. Those systems communicate across the organization, facilitate resource sharing, and provide ready access to information that personnel require to fulfill their responsibilities.

In addition to the physical and environmental controls described below, and as mentioned elsewhere in this report, Verisk is governed by mature policies and procedures that also function as operational safeguards in the day-to-day performance of its duties.

Physical Controls

Verisk's primary Data Centers in the United States, the EDC and WDC, are located in Somerset, New Jersey and Lehi, Utah, respectively. The WDC facility is owned by Verisk and operated by Verisk personnel. The EDC is hosted and co-located by the subservice provider, CyrusOne. Office space has been leased at a CyrusOne data center to enable Verisk to maintain personnel on-site and to maintain and monitor the environment more effectively.

In most cases where responsibility for a certain control has been assumed by a third-party service provider, this process has generally resulted in an enhancement within the control capabilities. The third-party colocation service providers are ISO 27001-certified and undergo annual SOC 2 audits.

In the Eastern, Western, and International Data Centers, access is restricted to authorized personnel only. The Data Centers' access controls include identification badges, personal identification numbers, and biometric security devices. Closed-circuit TV (CCTV) cameras record activity throughout the facilities. Using motion sensors and door contacts, alarm systems are monitored to detect and respond to any unauthorized access.

In the Eastern and International Data Centers, the colocation subservice providers are responsible for maintaining the access controls in their respective facilities. While the action of granting physical access is performed by the subservice provider, Verisk IT personnel are responsible for determining those individuals that should be granted access and for communicating required access changes (e.g., removal of access). Physical access to all of Verisk's Data Centers is reviewed and approved quarterly.

In an effort to eliminate single points of connectivity failure, the voice, point-to-point, and Internet circuits supplied to the Data Centers use various service providers, diverse physical paths, and diverse facility entry points.

The Data Centers are also equipped with uninterruptible power supply (UPS), battery backup systems, and redundant power distribution units. In the event of a power surge from the utility feeds, the UPS absorbs the surge, preventing it from passing to the Data Centers' infrastructure. In the event of a power failure, the UPS temporarily switches to the battery backup system while the generator starts up. At that time, power transfers from the UPS to the generator. The generator continues to provide power until the primary power source is restored.

The EDC and WDC use commercial-grade diesel generators which provide secondary power to the Data Halls. They are capable of providing enough power to sustain operations in the Data Centers for 72 hours before refueling is required. The generators are continually monitored using the following metrics: oil temperature, load, power output, and fuel consumption. Generators are run-tested monthly, and preventative maintenance is performed semi-annually. Specific refueling contracts are in place based on the geographic location of the Data Center.

While it should be noted that the generators and UPS battery backup systems for the EDC are maintained and tested by the co-location subservice provider, the information in the previous two paragraphs concerning generators and UPS systems is in place and maintained by the service provider. They provide redundant, highly available, and conditioned supply of power to the Data Hall. Verisk is responsible for maintaining the rack PDUs within the Data Hall, which supply redundant, highly available power to the equipment within the racks.

The International Data Centers have diesel engine generators in place to provide power to critical equipment. Base tanks provide 3,000 gallons of fuel storage and a minimum fuel storage sufficient for at least 12 hours of system uptime. The International Data Centers' subservice provider maintains and tests the generator and UPS systems and has a short notice refueling contract in place.

Environmental Controls

The EDC and WDC use a hot aisle containment system to control the temperature of the systems. The hot aisle containment system (HACS) encloses an aisle to collect the hot exhaust air from the equipment and cools it to make it available for the equipment air intakes. This process creates a self-contained system capable of supporting high-density workloads. To maximize efficiency and address the dynamic demands of the managed and hosted systems, air-conditioning units deliver chilled air to the Data Hall. The units actively adjust fan speed and chilled water flow to match the heat load. For the EDC, this system is monitored and maintained by the colocation subservice provider, CyrusOne.

The International Data Centers have zoned temperature control systems. They contain multiple HVAC units to verify correct temperature in critical areas. The average temperature within each area is maintained between 65- and 80-degrees Fahrenheit, as required for each area. If the temperature varies outside preset limits, an alarm is generated, and facilities personnel are notified.

Each Data Center is equipped with environmental sensors, including moisture sensors in the floor and ceiling, temperature sensors on the front and back of equipment racks (to measure input and output temperatures), and air humidity sensors (to provide real-time environmental monitoring). In the cases of the Eastern and International Data Centers, environmental controls are monitored and maintained by the respective co-location subservice provider.

Each Data Center is equipped with state-of-the-art fire suppression systems. Smoke and heat sensors detect potential fires. Fire detection systems are monitored 24/7/365. The systems communicate directly with the local fire departments.

Cloud Operations

Verisk systems are segmented into separate accounts and virtual private clouds (VPCs) in Amazon Web Services. The VPCs enable a fault-tolerant network topology. These services are available to Verisk businesses in six AWS regions worldwide in the United States, Europe, and Asia Pacific.

Managed Services' Cloud Operations team has established guidelines and leading practices in support of businesses building infrastructure in AWS. This model consists of a core infrastructure, a set of standard and reusable scripts for cloud deployments, and an application tier to enable the businesses to rollout systems in a controlled and transparent manner. The configurations of each application tier are subject to independent monitoring, risk assessments, and vulnerability mitigation.

Verisk's VIT Cloud Operations team manages the establishment, maintenance, and configuration monitoring of all AWS accounts and virtual private clouds (VPCs) for all Verisk business and functional units. Cloud Operations has implemented a formal set of reusable components and scripts to be used by the Verisk business and functional units to standardize their deployments to the cloud. It is intended to be used with an agile approach, supporting Continuous Integration / Continuous Delivery (CI/CD) in the cloud.

Cloud Operations, in collaboration with Verisk's Internal Audit team and Enterprise Risk Management, perform continual monitoring of the configurations of all accounts and VPCs against a standard set of parameters. Each account owner is notified on the status of the configurations on a monthly basis.

2. Software

Secure Configuration and Software Distribution Services

Managed Services uses several tools and related processes to standardize the server and desktop environment. The Global Workforce Support (GWS) team deploys changes to desktops. Initially, the teams send the packages to various desktops, where they test vital applications for continued functionality. Upon successful testing, the teams distribute the software packages to desktops during off-hours or on weekends. They track and report the status of package deployment.

The GWS team adhere to Standard Configurations for endpoints such as desktop or laptop computers. This process includes hardened images with end-point security, including media protection. Laptops use full-disk encryption software and media protection. Strong standards create a reliable, well-managed desktop environment protected from external threats.

The GWS team meets regularly to review security patches and upgrades to the environment. The team follows a predetermined schedule for applying patches to hardened systems.

The Global Security Services' Security Engineering team oversees scans of servers and workstations for unauthorized user accounts, server configuration, and unauthorized open ports on each device. Designated approvers from Mainframe and Distributed Infrastructure Support, as well as Information Security, review and approve configuration changes. Information Technology personnel follow industry practices and standards to secure server and workstation configurations, including account lockout policy, administrator accounts, password restrictions, disk partitions, registry settings, auditing, antivirus, and patches. Configured software includes the latest approved service packs, performance management tools, and antivirus software.

3. People

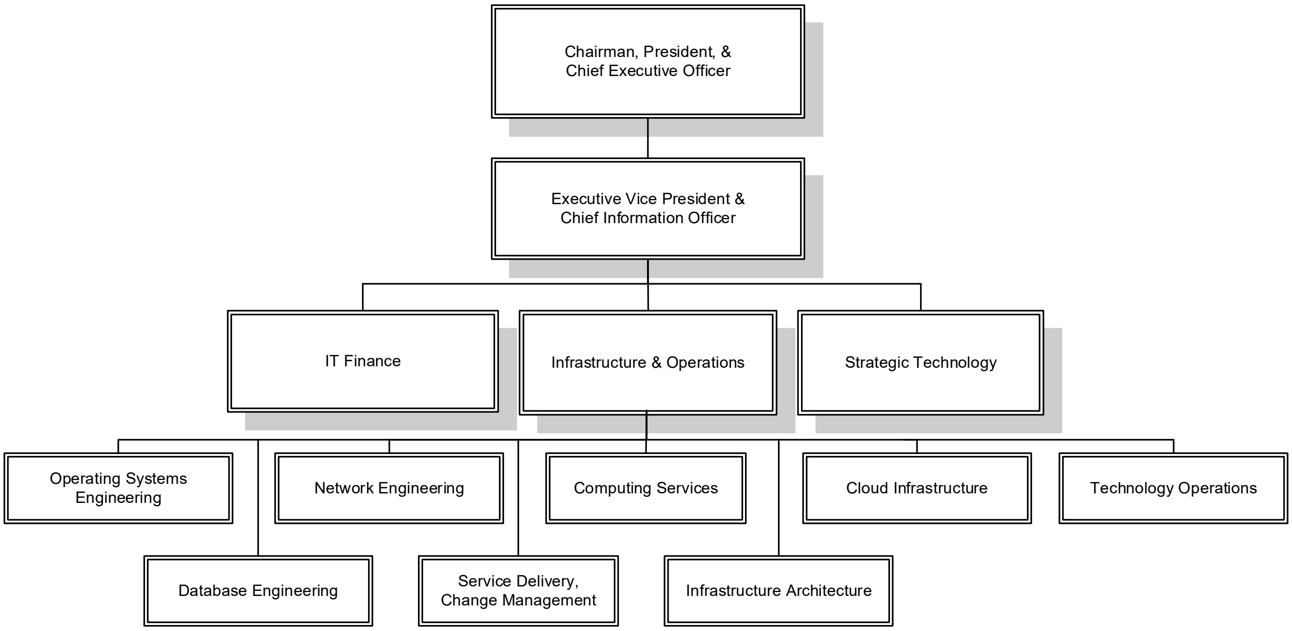
Organizational Control Environment

Verisk management has established – and Verisk's Information Technology management has adopted a control environment that sets the tone for internal activities and processes. Key elements of the control environment include:

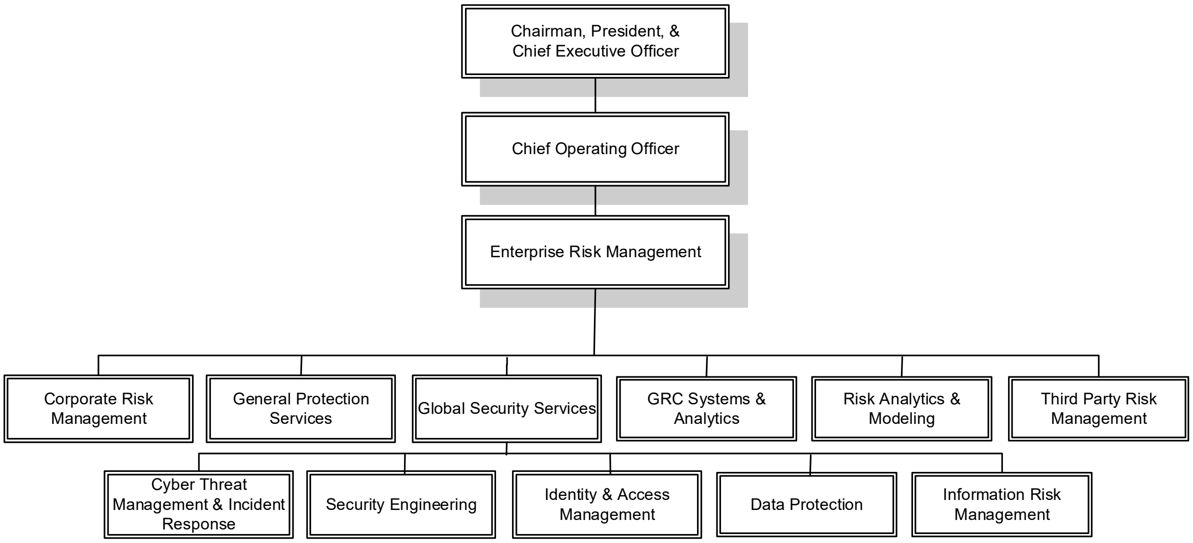
- Integrity and ethical values,
- Commitment to competence,
- Management's philosophy and operating style,
- Organizational structure,
- Assignment of authority and responsibility, and
- Human Resources policies and practices.

Organizational Structure

Verisk has implemented an organizational structure that promotes product quality and customer service. The Eastern, Western, and International Data Centers' management team consists of the Executive Vice President and Chief Information Officer and direct reports, as shown below.



Certain controls affecting Verisk's Information Technology are the responsibility of support units that report through the Executive Vice President, General Counsel, and Corporate Secretary to the Chairman, President, and Chief Executive Officer, as shown below.


Chairman, President, & Chief Executive Officer
Chief Operating Officer
Enterprise Risk Management
Corporate Risk Management
General Protection Services
Global Security Services
GRC Systems & Analytics
Risk Analytics & Modeling
Third Party Risk Management
Cyber Threat Management & Incident Response
Security Engineering
Identity & Access Management
Data Protection
Information Risk Management

Human Resources Policies and Practices

People Leadership and Culture is responsible for Verisk's Information Technology staffing; employee orientation and training; performance evaluations; compensation, recognition, and benefits; and administrative and employment-related programs, practices, and policies. People Leadership and Culture also manages the off-boarding activities, including conducting exit interviews, disabling user accounts, and collecting assets.

The staffing process begins with the vetting of applicants through multiple interviews, investigation of past employment, and confirmation of educational credentials. New hires must pass a pre-employment background screening that includes a criminal check. Some other positions may also include more extensive background checks depending on their job duties (e.g., finance-related roles may also receive a credit check, etc.).

New-employee orientation programs communicate policies on security, privacy, proprietary information, workplace harassment, equal employment opportunity, and employee conduct, in addition to other policies.

Performance evaluation is an annual process during which employees establish their goals and objectives, obtain supervisor input and approval, periodically assess their progress, update their goals for changing events, and receive formal evaluation from their supervisors at the end of the evaluation period. Evaluations drive employee compensation and advancement and identify areas for improvement.

Commitment to Competence

Having people with appropriate skill sets in each job is important for the effectiveness of a system of internal controls. Through years of experience, management has determined the experience, training, and competency levels required for the various job functions. Verisk's Information Technology (VIT) follow a documented hiring process in which the hiring manager develops the position description and works through human resource recruiters to find the right person.

An annual performance evaluation process confirms the maintenance of employees' skills and adherence to established policies and procedures. Each employee receives a review by his or her immediate supervisor. Supervisors document the evaluations using standard forms. Appropriate managers and executives subsequently review the forms. Performance evaluations link to compensation raises, bonuses, and remediation plans as appropriate.

VIT provides access to necessary training, including offerings that address change control, production support, security awareness, and other key areas. VIT also provides access to external training required to obtain or improve skills (for example, because of changes in products or environments), as needed.

Management's Philosophy and Operating Style

The Verisk Board of Directors sets high standards for employees, officers, and directors, and VIT has adopted those standards. Implicit in this philosophy is the importance of sound corporate governance. It is the duty of the Board of Directors to serve as a prudent fiduciary for shareholders and to oversee the management of the Company's business. To fulfill its responsibilities and to discharge its duties, the Board of Directors follows the procedures and standards set forth in the Corporate Governance Guidelines. The guidelines are subject to modification from time to time, as the Board of Directors deems appropriate in the best interests of the Company or as required by applicable laws and regulations.

The Corporate Management team is responsible for implementing management's philosophy and operating style. Everyone at Verisk – from its Chief Executive Officer to its newest employee – is guided by The Verisk Way™, a statement that reflects the Company philosophy. The core of The Verisk Way is three simple but powerful statements: Serve. Add Value. Innovate. Serve by anticipating the needs of its customers and colleagues and exceeding their expectations. Add Value by improving quality, productivity, and timeliness. Innovate by visualizing the future and being thought leaders.

Integrity and Ethical Values

VIT has adopted Verisk's programs and policies designed to promote and support integrity and ethical values within the organization. For example, Verisk requires all new employees to attend a multi-session orientation and to review the Employee Covenants and Privacy Policy (Covenants). The Covenants lay out employee responsibilities and establish management's expectations regarding various unacceptable activities and behaviors and the related penalties. The Covenants discuss the nature of information and the protection of information entrusted to Verisk. Each employee must sign an acknowledgement that he or she has read and understood the contents of the Covenants. People Leadership and Culture gives copies of the Covenants to new employees, and all employees can access them through the Company network as an ongoing reference for specific questions and issues. In addition, the Data Centers require employees to participate in annual training that addresses required control activities relating to privacy and security.

In the case of an ethical issue or other business issue arising, Verisk provides channels to communicate and resolve the issue without fear of retribution. The Whistleblower Policy encourages employees to voice their concerns. Verisk prohibits employees at all levels from taking retribution against anyone for reporting or supplying information about a policy concern. If an employee believes such retribution may have occurred, he or she may file a complaint with People Leadership and Culture, who fully investigate all such matters.

Assignment of Authority and Responsibility

The Data Centers' management team monitors progress toward achieving the Data Centers' goals. Management team members are responsible for developing plans to achieve the objectives assigned to them. The authority and responsibility to execute flows from the management team members to managers and line personnel.

The management team uses various methods of communication and control to help ensure that employees understand their individual roles and responsibilities as well as the authority carried by their positions and their ascending and descending reporting relationships. Methods include the following:

- Formal job descriptions;
- Documented policies and procedures;
- New hire orientation and training programs;

- Annual privacy and security training covering individual responsibilities for compliance with information privacy and security policies, protection practices, and procedures;
- Annual incident response training; and
- Group-specific employee training as well as instruction on the use of new products and services, as needed.

Cloud Operations Services

The Cloud Operations team, part of Verisk's Information Technology Department, has established standard practices to enable Verisk business units to set up their infrastructure in Amazon Web Services (AWS). The engineering, operational, and security related services performed by VIT extend to the cloud, including Identity & Access Management, Network Engineering, Compliance Monitoring, Configuration Management, Patch Management, Change Management, Business Resiliency, Data Protection, and Incident Response. All Verisk business units that own AWS accounts subscribe to these services.

4. Data

The Computing Services team is responsible for the arrival, acceptance, storage, and retrieval of data, and the delivery of results. The units oversee the quality of data from the point of receipt by the Data Center. The units also maintain data feeds and data stores which they regard as critical corporate assets, and expend considerable resources to help ensure their preservation, protection, quality, and management.

For information-based products, the following procedures assurance the quality of the data:

- Early and proactive review of data in the data processing system
- Incorporation of automated review of data to the fullest extent possible
- Efficient use of resources, including knowledgeable and experienced staff
- Full documentation of the data review process
- Documentation and reporting to internal users of anomalies found in data
- Thorough reviews of data, balanced against potential materiality of data anomalies and timeliness of product delivery
- Reviews based on objective criteria, as well as enhanced reviews by skilled and experienced staff using subjective criteria

There are three key steps in the lifecycle of statistical data:

- Arrival and acceptance
- Storage and retrieval
- Delivery of information-based products to external entities

Arrival and Acceptance

Data quality activities include field validity and field relationship edits; basic checks, such as balancing control totals; and additional checks, such as reasonability tests on aggregate data. In addition, the review process for aggregate data employs the judgment of actuaries and actuarial analysts familiar with insurance coverage and data as well as the external environment that can affect such data. The various data quality reviews help ensure the proper use and interpretation of the data in the downstream processing and development of information-driven products, such as loss costs.

Storage and Retrieval

The Data Center maintains infrastructure to store, compile, report, and deliver data to internal and external users. The company:

- Uses a structured method to update and enhance systems,
- Maintains strict controls on the database update process,
- Adheres to relevant privacy regulations,
- Employs covenants and policies to require employees to safeguard confidential data,
- Limits access to data to individuals based on need-to-know, and

- Incorporates hardware and data security software to protect access to data.

Delivery of Data Products to External Entities

Production Services follows strict procedures in the delivery of products. IT Technology Operations validates that each customer is entitled to each product before product delivery.

5. Policies and Procedures

Risk Assessment

Verisk's Executive Risk Management Committee (ERMC) is responsible for setting a strong tone at the top that risk management is a critical responsibility of all managers across the organization. The ERMC provides guidance and authority related to the enforcement of the Company's enterprise-wide risk management framework and Enterprise Risk and Compliance (ERC) function, including the strategies, policies, procedures, processes, and systems established by management to identify, assess, measure, monitor, and manage the major risks facing the Company.

VIT has governance processes built on the risk management framework that leverages the NIST 800-30 risk management framework across all of the business units. The framework identifies, analyzes, and assesses the potential effects of unplanned events. Verisk adopts risk mitigation strategies to reduce residual risk to an acceptable level. The risk assessment considers the risk tolerance of key stakeholders of the Data Centers.

The principal elements of the risk management framework include the following:

- Information technology and business risk management,
- Event identification,
- Risk assessment,
- Risk response, and
- Maintenance and monitoring of risk action plans.

In the event that extenuating circumstances prohibit full compliance with Verisk policies, the business must file for policy exceptions and acceptance of the underlying risk conditions. These exceptions require formal review and approval by the Business Unit Executive. In the event that the risk is considered material or if the operating risk is high, then the exception must be approved by the ERMC. Exceptions will only be approved for a specified period of time, not to exceed 12 months.

Information Technology and Business Risk Management

The Verisk Data Centers have established an integrated information technology governance, risk management, asset management, and control framework within their risk management framework. This process includes alignment with the organization's risk tolerance level.

Event Identification

The Data Centers' management team identifies events that may affect the goals or operations of the enterprise and considers business, regulatory, legal, technology, trading associate, human resources, and operational aspects.

Information Risk Assessment

Annually, the Information Risk Management team assesses the likelihood and effects of all identified risks, using qualitative and quantitative methods. The team determines the likelihood of each identified risk as well as the potential effects of inherent and residual risks.

Risk Response

The Information Risk Management team maintains a risk response process that identifies a risk owner and affected process owners. The process helps to ensure that cost-effective controls and security measures continually mitigate exposures to risk. Risks are managed by the risk and process owners using one or more of the following methods:

- Terminate – Eliminate, withdraw from, or do not become involved in an activity creating risk.
- Take – Accept the risk and plan for the expected impact.

- Transfer – Move the risk to another party by hedging against undesired outcome or reduce the risk through processes such as insurance.
- Treat – Control the risk through additional or optimized controls.

Maintenance and Monitoring of Risk Action Plan

The Information Risk Management team prioritizes and plans control activities to implement risk responses and to identify costs, benefits, and responsibilities for execution. The Data Centers' management team assesses all identified risks for recommended actions and acceptance of any residual risk. The team monitors execution plans and reports deviations to management.

Control Monitoring

To help determine the effectiveness of internal controls, the Data Centers' management team performs regular, ongoing monitoring, as well as separate evaluations. Monitoring includes:

- Data Center Operations: Using a variety of automated tools, Data Center Operations performs continuous monitoring of applications, networks, system availability, and performance.
- Independent Control Evaluations: External firms and Internal Audit provide independent testing of the design and operation of controls.

For example, Verisk maintains an Information Security Management System (ISMS) that is ISO 27001:2013-certified for Managed Services over Verisk's EDC and WDC, as well as their management of Verisk's AWS VPCs. The certification requires external, independent audits of controls that illustrate a continuously improving ISMS. Controls assessed include policies, procedures, and technical measures implemented to secure the environments. Maintenance audits are performed annually, and certifications are awarded on a three-year cycle.

Internal Audit is an independent and objective appraisal function that examines and evaluates the activities of Verisk. Internal Audit reports functionally to the Audit Committee of the Board of Directors and administratively to the Executive Vice President, General Counsel, and Corporate Secretary. Internal Audit performs scheduled internal control reviews of the Data Centers including:

- Information technology general control audits,
- Pre-implementation consulting reviews of significant technology and infrastructure implementations,
- Integrated audits of critical business processes,
- Information technology security and privacy reviews, and
- Audits of other technology services.

System Development Lifecycle

Development

Software development activities are carried out and managed at the business level, not at the Data Center level. Each of the operational business units is responsible for the design, development, and testing of its respective applications. Once sufficient testing is completed, all changes are passed through User Acceptance Testing (UAT). Upon completion of UAT, changes and updates are packaged and submitted for approval via the Change Management Services Program. Once proper authorization is provided, testing completed, and data owner approval is obtained, the Software Configuration Management team will move the changes into production.

Change Management Services

The Change Management team is responsible for providing a platform for technical and business teams to document their changes to production systems that affect IT services. The Change Management team's purpose is to help ensure that all changes are documented and recorded with the appropriate risk impact and that appropriate approvals are in place. The Change Management team provides guidance on the Change Management process.

Key elements that make the Change Management function effective include:

- Formal standards and tools and
- Trained and qualified staff.

Formal Standards and Tools

Change Management leverages ServiceNow to help ensure that all changes to production are documented, recorded, and completed as intended and within the guidelines of the Change Management Policy.

Trained and Qualified Staff

Managers of the staff performing the changes are required to sign off and approve the content of all changes prior to their implementation. The reviewing manager confirms that the content of each change, including the implementation plan, test plan, and backout plan are accurate, complete, and scheduled at the appropriate time.

Global Security Services

Access Provisioning, De-provisioning, and Access Reviews

The ERM Global Security Services' Identity and Access Management team oversees logical access to computer resources, including applications, networks, and infrastructures. Team members process requests for new and modified access to resources. The respective resource owner, along with the requestor's supervisor, authorizes resource requests. Resource owners grant access based on need-to-know and commensurate with job responsibilities.

Upon termination of an employee or contractor, the department manager and Human Resources notify Identity and Access Management, which immediately disables access. In addition, the team re-evaluates employee and contract access levels upon change of job responsibilities. Owners and department managers confirm access to critical production systems via a recertification process on a quarterly basis. Additionally, Data Center management reviews physical access to the EDC and WDC quarterly.

Resource Owners

Resource Owners report to and are empowered by their respective Business Executive with full accountability for the business unit's segment of products and services. Their responsibilities include:

- Maintaining an awareness of the sensitivity and classification of the data they handle, as well as the laws and regulations associated with protecting the information/data.
- Defining, describing, and classifying all data in their respective lines of business.
- Determining and authorizing appropriate access rights to the application systems and data resources supporting their products and services.
- Approving access requests and periodically validating access permissions to the application systems and data resources.

Information Security

The Data Centers follow the Verisk Information Security Policy Framework and aligned policies to protect the integrity and confidentiality of information, products, and computing facilities. The policy is based on the ISO 27001 and NIST 800-53 frameworks covering data security; communications security; software use and virus protection; intellectual property and privacy rights; encryption; backup, archival storage, and disposal of data; physical security; systems contingency planning; and contingency planning and disaster recovery. Senior management is responsible for annual policy reviews and policies are revised, if necessary.

The ERM department oversees an awareness program that encompasses both security and privacy practices. The program increases individuals' knowledge of the vulnerabilities and consequences that may result from an information security breach. The awareness program also reinforces other privacy and security policy requirements to safeguard information. ERM personnel possess Certified Information Systems Security Professional certifications, privacy certifications, and other industry-recognized certifications.

Privacy Notice

User entities (customers and information suppliers) collect personal information and are responsible for providing privacy notices to individuals. User entities are responsible for determining the consents, authorizations, legal bases, and other documentation required to collect personally identifiable information and protected health information. The Data Centers do not interact directly with the individuals to whom such personal information relates and therefore, are not responsible for providing such notice.

Verisk's Statement of Security and Privacy Practices

Verisk is committed to protecting the privacy and confidentiality of consumer and patient information transmitted to and maintained by the Company. The policies and procedures have been designed to meet or exceed the physical and electronic security measures required by applicable federal and state regulatory guidelines for the use, storage, and/or transmission of such information. Verisk has implemented electronic and physical security measures and established administrative security procedures to protect the information from unauthorized access, improper use, alteration, and unlawful or accidental destruction. Verisk adheres to applicable laws, including the privacy and security regulations promulgated pursuant to the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (including the Health Information Technology for Economic and Clinical Health [HITECH] Act of 2009 and as updated via the Final Omnibus Rule of 2013), and any modifications of those acts. Each business unit is responsible for operating within and adhering to the privacy and security regulations it falls under.

Dedicated Service Desk Support

The Service Desk provides technical and business support for internal customers. The unit's mission is to give customers the highest-quality support while exercising cost-effective practices.

The Service Desk prioritizes calls according to their severity and effect. Management establishes and closely monitors performance on service-level objects.

Business Continuity and Disaster Recovery Services

The ERM group oversees the development of a coordinated business continuity and disaster recovery plan to enable proper action before, during, and after an emergency affecting the Data Centers. The plans help to ensure that the transition to the business continuity plan and/or disaster recovery plan is seamless and that service to customers will continue to meet expected levels. Business continuity management is the responsibility of the ERM team, which reports to the Executive Vice President, General Counsel, and Corporate Secretary.

The plans maintain critical operations in the event of a major disaster. Although the types of possible disasters are too numerous to list, there are five general scenarios:

- *Localized Disaster*: A disaster, such as a fire, destroys all or part of the building. Such a disaster may require partial or even total relocation of business operations to an alternative site.
- *Denial of Access*: The building and contents are intact but inaccessible. A nearby hazardous materials event, lack of water or power, or an occurrence of workplace violence would cause such a situation.
- *Worse Case*: A localized disaster destroys a Data Center facility and all of its contents but does not affect customers.
- *Regional Disaster*: A widespread disaster affects both the Data Center and surrounding area.
- *Pandemic*: A contagious disease occurs over a widespread area and affects a high proportion of the population.

Business continuity and disaster recovery plans cover the worst-case scenario on the premise that recovery teams use parts of the plans to respond to less severe interruptions. The teams test the plans based on a variety of scenarios.

A response consists of three distinct phases – emergency response, recovery, and restoration – each with its own set of objectives. The duration of each phase depends on the nature of the event and its effect on business processes and applications.

- *Emergency Response:* During the unfolding of an event, the organization first takes action to protect life and property. After that, the priority shifts to mitigation of damages, preservation of property, and initial assessment of the effects. The Recovery Management team decides whether to declare a disaster, based on the event's effect on critical business functions, applications, customers, and other third parties.
- *Recovery:* As soon as the Recovery Management team declares a disaster, efforts to recover from it begin. The objective of recovery is continuation of functions and applications to support customers and critical internal operations. The phase continues until restoration of the Data Center facility is complete and operations are ready to return to normal.
- *Restoration:* The organization performs the tasks required to rebuild damaged facilities and restore original business functionality. Restoration runs concurrently with recovery operations.

Business Continuity management, in coordination with the business units, conduct at least one annual production recovery simulation. In addition, a series of smaller tests occur every year. Those tests include:

- Administrative review of plan procedures,
- Paper tests ("tabletops") to gauge participants' understanding of roles and responsibilities, and
- Partial tests of recovery capabilities at the recovery site.

The Verisk Information Technology teams select and implement a disaster recovery testing strategy with appropriate yearly objectives. The organization selects specific tasks to highlight changes in procedures, hardware, and other components not recently tested. Verisk has contracted with a third-party, CyrusOne, to provide the infrastructure and equipment necessary for testing and in the event of a disaster at the EDC. The services include network connectivity, infrastructure, processors, servers, storage, distributed systems, and workstations. The EDC is the primary disaster recovery site for the WDC, while the backup location for the International Data Center is a warm site located in Germany.

<u>Backup Services</u>

All servers, including mainframes, are configured to complete daily backups by replicating files on storage devices at the alternate site (i.e., Eastern Data Center replicates to the Western Data Center and vice versa). Infrastructure operations receives reports of any failed backups. All servers, including mainframes, are configured to complete backups in accordance with a defined schedule. Infrastructure operations receives reports of any failed backups.

Managed Services' IT Operations team maintains an internal replication network to perform replication between the EDC and WDC. The teams send backups of mainframe and distributed systems, as well as incremental daily encrypted backup tapes, to a secure third-party off-site facility. In addition, the teams securely transmit second copies of the distributed server backups over a dedicated line to the recovery center. Only authorized personnel can request tapes from the off-site facility. In an emergency, the service provider will securely package tapes in locked containers and transport them to the recovery site within approximately three hours.

<u>"Defence-in-Depth" Protection Services</u>

To protect against unauthorized access to the systems, management has designed and implemented a layered approach to network security controls. The approach includes:

- Securing the perimeter,
- Intrusion detection,
- Maintenance,
- Access provisioning, and
- Monitoring.

For early identification of potential security breaches, an intrusion detection system provides continuous monitoring of the network. The intrusion detection system uses a detection engine and event correlation technology to identify suspicious traffic patterns that may indicate a network compromise or other network-based threat. Controls include a traffic-pattern normalization process, constant monitoring, monthly reporting, and annual tuning, as necessary. The IT Services Operations teams monitor network intrusion detection system alerts.

Firewalls protect the Internet-facing infrastructure and applications. The firewalls restrict access between networks and allow access only to specifically configured services. Multiple firewall devices at the access points into the network prevent intrusion, limit accessible services, and isolate the network from those of customers and other third parties. In addition, there are firewalls between demarcation zones and the internal network.

To protect against malware and viruses, software tools are deployed to filter inbound Internet traffic for malicious content, including virus vectors. An e-mail service removes spam messages and quarantines potentially malicious e-mails. When available, a protocol, called transport layer security, encrypts e-mail communications. Verisk's Information Technology teams receive and transmit data only through encrypted or physically secured channels.

To prevent data leakage, encryption protects the confidentiality and integrity of information owned by and entrusted to the Data Centers. Secure sockets layer, transport layer security, secure file transfer protocol, and Pretty Good Privacy (PGP) technologies encrypt information in transit. Mobile devices – including laptops, notebooks, and smartphones – are deployed with full disk encryption. In addition, tape drives encrypt data sent off-site for archiving purposes.

Incident Management Services

Verisk has fully functional incident response units, which identify, resolve, and determine the root cause of outages. The manual or automated creation of a problem ticket notifies the unit of system outages. For each ticket, the system or a person assigns a severity level. The incident management system notifies the Service Desk and Technical Operations Center of severity 1 and 2 tickets all day, every day. Incident Management oversees the following incident security levels:

Severity	Western and International Data Centers	EDC	Response SLA	Responsibility
1	Customers are unable to access an entire production system or application, regardless of data source or support responsibility.	Customers are unable to access an entire production system or application, regardless of source or support responsibility.	1 hour	IT Services Operations / Service Desk
2	Customers are unable to access part of a production system or application or are experiencing response issues.	Customers are unable to access part of a production system or application or are experiencing response issues.	4 hours	IT Services Operations / Service Desk
3	An application or part of the infrastructure is at risk of a severity 1 or severity 2 incident if not treated within a known period.	An application or part of the infrastructure is at risk of a severity 1 or severity 2 incident if not treated within a known period.	24 hours	Support group for affect area

In addition to identifying and resolving system outages, the automated incident management system also supports response to security incidents. For such incidents, a Security Response team of trained first responders immediately investigates the report. This team identifies, assesses, and resolves both security- and privacy-related incidents. They use industry-standard forensic techniques to evaluate, investigate, and determine the root causes of suspected unauthorized intrusions. For each identified security incident, the team assigns a severity level based on two major categories:

- Consumer information
- Customer information

Based on the type of breach and its severity, the Senior Vice President of ERM informs the Chief Internal Auditor and the Executive Vice President, General Counsel, and Corporate Secretary of the findings, conclusions, and recommendations.

Cloud Team Services (Services provided by Verisk Managed Services and the Verisk Cloud Security Team)

1. **Availability/Monitoring**

   AWS availability and monitoring is overseen centrally by the Verisk Cloud Security team. The organization uses various tools for availability/monitoring. Actions to perform when a violation is discovered varies based upon severity and can range from informational reporting to immediate altering, to immediate corrective action. To monitor for availability, the organization uses CloudWatch. CloudWatch collects operational data in the form of logs, metrics, and events; this process provides Verisk with a unified view of AWS resources, applications, and services.

ClaimSearch® (Services provided by the ClaimSearch® Business Unit)

1. **Infrastructure**

   The ClaimSearch® environment that is managed through AWS is logically partitioned from all other, non-ClaimSearch® corporate environments, systems, and services. Only designated Verisk employees can access the ClaimSearch® Platform.

   AWS

   Architecture and System Design: The ClaimSearch® Platform utilizes the AWS Infrastructure-as-a-Service (IaaS) and is required to adhere to related Verisk and ClaimSearch® policies as outlined within the description section of this report. Additionally, AWS IaaS design and architecture are reviewed by the Verisk Security Architecture Review Board (SARB), consisting of senior leadership within the Information Security department and appropriate business units. Changes impacting the architecture must undergo additional review through the SARB.

   AWS services/tools: VPC (Virtual Private Cloud), Lambda, S3, API Gateway, EC2, Elastic Container Service (ECS), Aurora Postgres (RDS), DynamoDB, VPS, CloudTrail, Route53, CloudFormation, Config, IAM, Simple Notification Service (SNS), Systems Manager, CloudWatch, Application Load Balancer, AWS Certificate Manager, AWS CloudFront, Auto Scaling, Direct Connect, Trusted Advisor, SQL Server, Secrets Manager, Guard Duty, Amazon MQ, Glacier, Workspaces, SQS, AWS Batch, Glue, Macie, and Step Functions.

   Ongoing monitoring: AWS SOC 2 reports are reviewed at the enterprise level no less than annually in accordance with the Company's standard operating procedure to help ensure appropriate controls, system availability, processing, integrity, and confidentiality of all data being processed by ClaimSearch® through AWS systems.

   Storage and Retrieval: Verisk uses Commvault and RDS Snapshots for storage and retrieval of systems hosted in the AWS Cloud. Commvault and RDS Snapshots is used in the following regions: (1) US-East-2, (2) US-West-2, (3) EU-WEST-1, and (4) AP-Southeast

Information Security: To provide assurance that Verisk information security policies are enforced in the cloud; automated monthly updates of base images for supported operating systems are deployed. An automated process runs from the management account across all accounts and regions where required. The latest public Amazon Machine Image (AMI) adds Verisk security standards such as volume encryption, application of latest OS patches and hardening settings, Endpoint security agent installation, Centrify agent installation (for Linux) and saves as private encrypted AMI(s) in each Business Unit (BU) account. Verisk also utilizes customized centrally configured checks to help ensure compliance with security leading practices and/or Verisk policy with alerting, reporting, and where appropriate, immediate corrective action. Custom AWS Config rules are configured to check against a DynamoDB table in shared services where known exceptions to various policies are stored and periodically reviewed and re-certified. Actions to perform when a violation is found varies based upon severity and are detailed in documentation. They can range from informational reporting, to immediate alerting, to immediate corrective action.

2. Software

Delivery of Data Products to External Entities

Software development activities are conducted and managed at the business level. Each of the operational business units is responsible for the design, development, and testing of its respective applications. Once sufficient testing is completed, all changes are passed through quality assurance (QA) testing. Upon completion of the QA testing, changes and updates are packaged and submitted for approval through the Change Management Services Program.

Formal Standards and Tools

To meet stringent goals, Change Management is responsible for reviewing and approving changes that are scheduled to be promoted into production. The team follows a standardized process to help ensure that changes are implemented into production in accordance with the Change Management Policy.

Change Management leverages multiple system tools to help ensure that all changes to production are documented, recorded, and completed as intended and within the guidelines of the Change Management Policy.

Trained and Qualified Staff

The Change Management staff brings a combination of diverse and valuable skills to the organization. A Change Advisory Board governs the team. The Change Advisory Board reviews all infrastructure changes and assures that all guidelines are being followed. This group represents all infrastructure and most development teams. The board is responsible for reviewing and assessing the impact of all changes.

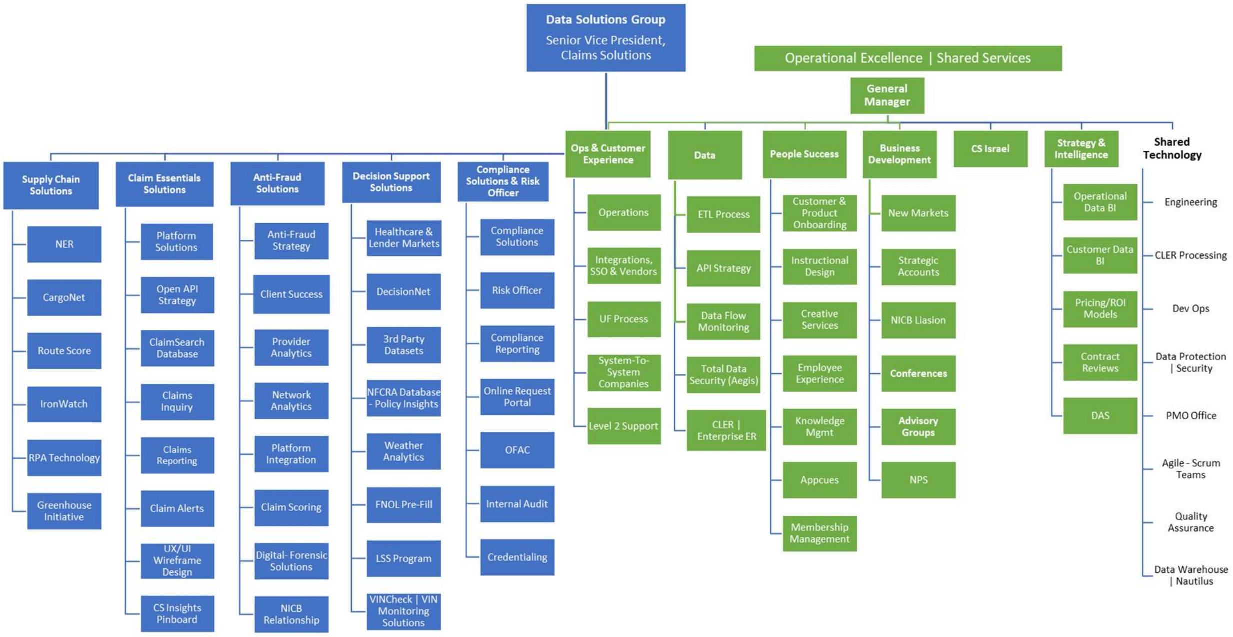
The Change Management lead participates on project teams and helps achieve the highest quality in final products. The Change Management lead is responsible for helping to ensure that testing is performed before approval of a change and that all packages are completed as part of the approval process.

In addition, Verisk has a Security Architecture Review Board (SARB), consisting of senior leadership within the Information Security department and appropriate business units. Changes impacting architecture must undergo additional review through the SARB.

3. People

Organizational Structure of ClaimSearch®

During the scope of this report, the ClaimSearch® management team consisted of the senior vice president of Claims Solutions, the Vice President and General Manager of ClaimSearch® Solutions, and direct reports, as shown below.



ClaimSearch® maintains a staff of approximately 190 individuals divided among the following departments:

- IT Development
- IT Production
- Claim Essentials
- Anti-Fraud Solutions
- Decision Support Solutions
- Compliance Solutions & Risk
- Operational Excellence
- Client Support
- Accounting
- Sales

At the business unit level, ClaimSearch® has key staff responsible for supporting business functions and operations while enforcing compliance with Verisk policies and procedures, as well as applicable legislation.

4. Data

Participating organizations must designate to ClaimSearch® at setup the way they wish to access the system. All data transmissions from the customer to ClaimSearch® and from ClaimSearch® to the customer are secured and encrypted in each of these options.

ClaimSearch® participating organizations use the supported transmissions to contribute their claims data to ClaimSearch®. All claims data records are assigned unique membership codes and unique identifiers to the record. Claims data is then matched based on unique attributes and returned to ClaimSearch® participating organizations via the supported transmissions. All sensitive data entering and leaving the ClaimSearch® Platform is encrypted. In addition, data at rest is encrypted within the Data Centers and AWS. ClaimSearch® maintains a Privacy and Security Policy with all ClaimSearch® participating organizations to help ensure the use and security of the sensitive data entering and leaving the environments. The below descriptions outline the specific point at which end users and participating organizations are notified of data successfully being stored within the database.

- *Secure web portals:* ClaimSearch® accepts data within the database upon successful submission notice through application accompanied by notice to the end user of success.
- *Web services (XML):* ClaimSearch® accepts data within the database confirming via echo return file.
- *SAML single-sign-on:* ClaimSearch® accepts data within the database confirming via echo return file.
- *SFTP:* ClaimSearch® accepts data within the database confirming via echo return file.
- *FTP with PGP encryption:* ClaimSearch® accepts data within the database confirming via echo return file.
- *MQ to API:* ClaimSearch® accepts data within the database confirming via echo return file.

If a member submits a record with “no search” upon receipt, an echo return file will not be submitted because no search was requested.

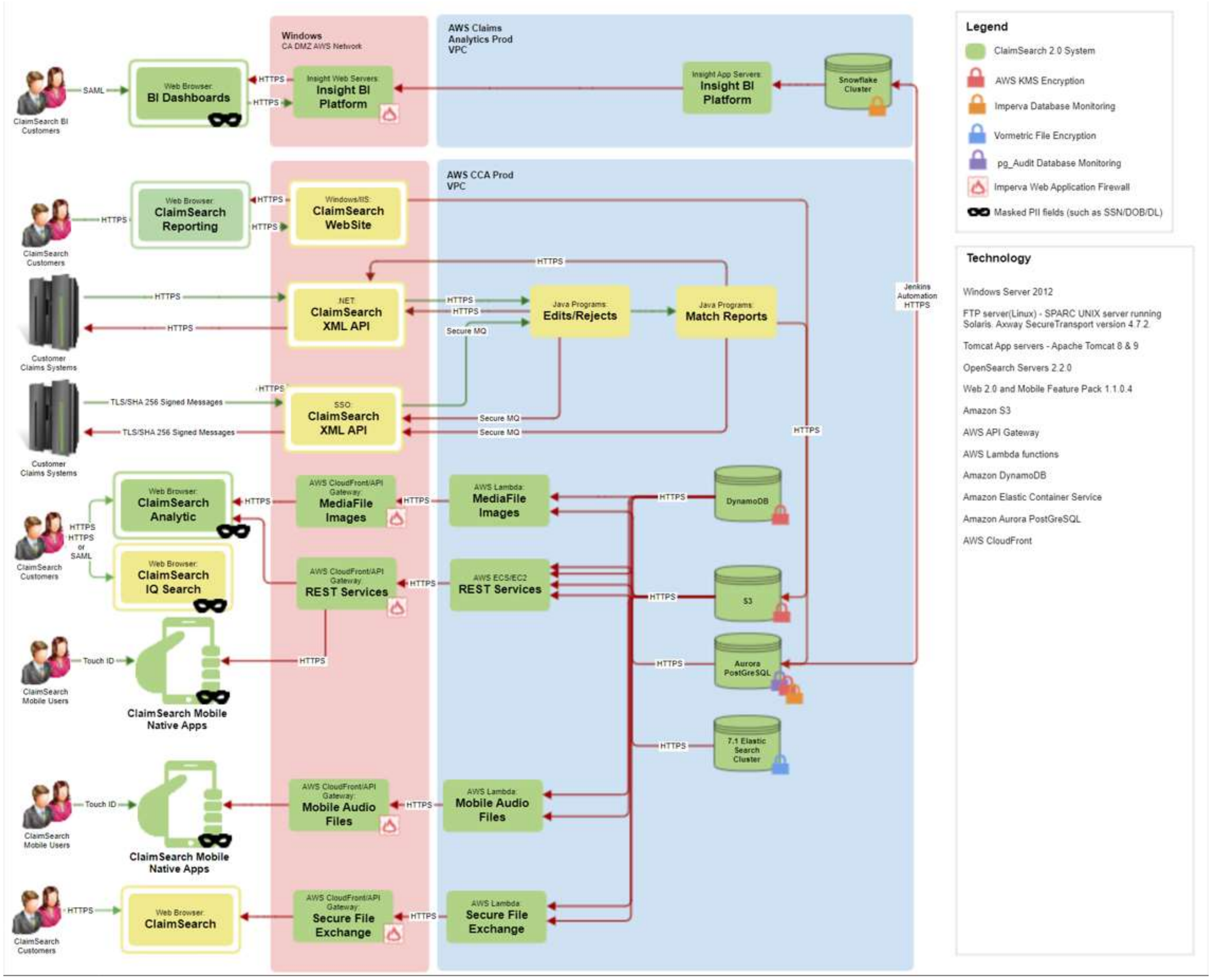
The classification of all data received, processed, produced, and stored by Verisk and its member companies is vital in determining what baseline processes and mechanisms are appropriate for safeguarding that data. Data shall be classified as to its sensitivity to the organization and security controls shall be applied accordingly. Data shall be labelled and handled in line with its classification. Data Owners or their assigned delegates evaluate and assign appropriate classification based on the value and sensitivity of the information in accordance with Verisk’s Data Classification and Handling Policy.

Data Quality Standards and Practices

The Verisk Production Services team is responsible for the arrival, acceptance, storage, and retrieval of data and the delivery of results. The units oversee the quality of data from the point of receipt by the Data Center. The units also maintain data feeds and data stores, which they regard as critical corporate assets, and expend considerable resources to help ensure their preservation, protection, quality, and management.

- For information-based products, the following procedures assure the quality of the data:
  - Early and proactive review of data in the data processing stream;
  - Incorporation of automated review of data to the fullest extent possible;
  - Efficient use of resources, including knowledgeable and experienced staff;
  - Full documentation of the data review process;
  - Documentation of anomalies found in data and reporting of such anomalies to internal users;
  - Thorough reviews of data, balanced against potential materiality of data anomalies and timeliness of product delivery; and
  - Review based on objective criteria, as well as enhanced review by skilled and experienced staff using subjective criteria.

- There are three key steps in the life cycle of statistical data:
    - Arrival and acceptance
    - Storage and retrieval
- Delivery of information-based products to external entities ClaimSearch® Data Flow


Windows
CA DMZ AWS Network
AWS Claims Analytics Prod VPC
AWS CCA Prod VPC
ClaimSearch BI Customers
SAML
Web Browser: BI Dashboards
HTTPS
HTTPS
Insight Web Servers: Insight BI Platform
Insight App Servers: Insight BI Platform
Snowflake Cluster
ClaimSearch Customers
HTTPS
Web Browser: ClaimSearch Reporting
HTTPS
HTTPS
Windows/IIS: ClaimSearch WebSite
HTTPS
Customer Claims Systems
HTTPS
HTTPS
.NET: ClaimSearch XML API
HTTPS
HTTPS
Secure MQ
Java Programs: Edits/Rejects
Java Programs: Match Reports
Jenkins Automation HTTPS
Customer Claims Systems
TLS/SHA 256 Signed Messages
TLS/SHA 256 Signed Messages
HTTPS
SSO: ClaimSearch XML API
Secure MQ
Secure MQ
HTTPS
ClaimSearch Customers
HTTPS
HTTPS
or
SAML
Web Browser: ClaimSearch Analytic
HTTPS
AWS CloudFront/API Gateway: MediaFile Images
HTTPS
AWS Lambda: MediaFile Images
HTTPS
DynamoDB
Web Browser: ClaimSearch IQ Search
AWS CloudFront/API Gateway: REST Services
HTTPS
AWS ECS/EC2 REST Services
HTTPS
S3
ClaimSearch Mobile Users
Touch ID
HTTPS
ClaimSearch Mobile Native Apps
HTTPS
Aurora PostGreSQL
HTTPS
7.1 Elastic Search Cluster
ClaimSearch Mobile Users
Touch ID
ClaimSearch Mobile Native Apps
AWS CloudFront/API Gateway: Mobile Audio Files
HTTPS
AWS Lambda: Mobile Audio Files
ClaimSearch Customers
HTTPS
Web Browser: ClaimSearch
AWS CloudFront/API Gateway: Secure File Exchange
HTTPS
AWS Lambda: Secure File Exchange
Legend
ClaimSearch 2.0 System
AWS KMS Encryption
Imperva Database Monitoring
Vormetric File Encryption
pg_Audit Database Monitoring
Imperva Web Application Firewall
Masked PII fields (such as SSN/DOB/DL)
Technology
Windows Server 2012
FTP server(Linux) - SPARC UNIX server running Solaris. Axway SecureTransport version 4.7.2
Tomcat App servers - Apache Tomcat 8 & 9
OpenSearch Servers 2.2.0
Web 2.0 and Mobile Feature Pack 1.1.0.4
Amazon S3
AWS API Gateway
AWS Lambda functions
Amazon DynamoDB
Amazon Elastic Container Service
Amazon Aurora PostGreSQL
AWS CloudFront

5. Policies and Procedures

Access Management

Only participating organizations may access ClaimSearch®. Further, only authorized users from those organizations may access claims information on behalf of the participating organization. ClaimSearch® requires participating organizations to comply with credentialing procedures. The NICB maintains the responsibility to credential NICB participating organizations. Organizations that have not successfully completed the credentialing process will not be allowed to access ClaimSearch®. Participating organizations are responsible to train authorized users and inform them of the importance of the data and the necessity of securing it. Participating organizations shall inform their respective workforce members and agents of the nature and scope of their participation in ClaimSearch®, together with all applicable laws, regulations, and other limitations.

Participating organizations shall review the backgrounds of their authorized users to assure that only qualified authorized users have access to the system. Further, Verisk reserves the right to deny access to any person or entity when it determines, in its sole and exclusive discretion, that such access would not be in its corporate interests or in the public interest. The NICB reserves the right to deny access to NICB-managed and controlled data accessible through ClaimSearch®.

IDs and passwords enable each user to access ClaimSearch®. A password reset requires the authorized user to answer knowledge-based security questions. Passwords must be eight characters, must contain at least one letter and one number, and may include special characters. The ClaimSearch® application forces a password reset once every 90 days.

Authorized users' access to and use of ClaimSearch® are monitored through up-front application controls in addition to threat monitoring. ISO Services, Inc. conducts workforce background checks for all employees. Verisk has the option to conduct audits with its own personnel, jointly with NICB personnel, jointly with participating organization personnel, or with participating organization personnel acting according to Verisk instructions.

Internal users must complete an official request process prior to being granted access to the ClaimSearch® system. Access request forms must be completed by users' managers and approved by senior management before access is provisioned. Privacy and security training is mandatory to obtain access to the database. Access is subject to quarterly recertification and subject to deprovisioning of terminated employees.

Logical Access Provisioning and Deprovisioning

The Verisk Service Desk team oversees logical access to computer resources including applications, networks, and infrastructures. Team members process requests for new and modified access to resources. The respective resource owner, along with the requestor's supervisor, authorizes resource requests. Resource owners grant access based on need to know and commensurate with job responsibilities. Upon termination of an employee or contractor, the department manager and Human Resources notify the Security Administration team, which removes access. In addition, the team reevaluates employee and contractor access level upon change of job responsibilities. Owners and department managers confirm access quarterly.

ClaimSearch® application access is provisioned and managed externally by member companies as outlined in the ClaimSearch® Privacy and Security Policies. User access is periodically reviewed by ClaimSearch® Compliance audit teams. Access management by member companies is managed through self-administration features that eliminate the requirement and need for participating organizations to contact the Verisk Help Desk regarding access. Just as with Verisk resources, ClaimSearch® follows industry best practice standards in provisioning internal access and expects member companies to hold to those same standards.

Change Management Services

The Change Management team is responsible for approving the final elements of all changes set to be implemented to production systems that affect IT services. The Change Management team's purpose is to help ensure that standard procedures are followed, all changes are documented and recorded, and overall business risk is minimized. The Change Management team provides guidance on the Change Management process.

Key elements that make the Change Management function effective include:

- Formal standards and tools
- Trained and qualified staff

Information Security

The Data Centers and ClaimSearch® support follow the Verisk Analytics Information Security Policy to protect the integrity and confidentiality of information, products, and computing facilities. The policy is based on the ISO 27000 standards and NIST 800-53 frameworks covering data security; communications security; software use and virus protection; intellectual property and privacy rights; encryption; backup, archival storage, and disposal of data; physical security; systems contingency planning; and contingency planning and disaster recovery. Senior management is responsible for security program implementation reviews and, if necessary, revises the policy.

The Risk Management and Compliance departments oversee an awareness program that encompasses both security and privacy practices. The program increases individuals' knowledge of the vulnerabilities and consequences that may result from an information security breach. The awareness program also reinforces other privacy and security policy requirements to safeguard information. Risk and Compliance personnel possess Certified Information Systems Security Professional certifications, privacy certifications, and other industry-recognized certifications.

The ClaimSearch® Compliance team releases periodic awareness notices on the best practices for ClaimSearch® usage, general data handling, and other developing compliance and information security topics. All ClaimSearch® users must also undergo ClaimSearch® privacy and security training to activate granted accounts.

Privacy Notice

ClaimSearch® provides a Citizen Inquiry process that permits an individual to review his or her claims history within ClaimSearch® as a requirement of the NAIC's Insurance Information and Privacy Protection Model Act and to assure the accuracy of the data. Participating organizations and authorized users direct all requests for information to ClaimSearch® through the ClaimSearch® Compliance unit.

Program support personnel continually monitor state and federal requirements stemming from laws on data breach notification and other privacy-related requirements. They implement appropriate updates to the Incident Response Plan and train staff as compliance requirements change.

Verisk's Statement of Security and Privacy Practices

Verisk Analytics and ClaimSearch® are committed to protecting the privacy and confidentiality of consumer and patient information transmitted to and maintained by the Company. The policies and procedures meet or exceed the physical and electronic security measures required by applicable federal and state regulatory guidelines for the use, storage, and/or transmission of such information. Verisk has implemented electronic and physical security measures and established administrative security procedures to protect the information from unauthorized access, improper use, alteration, and unlawful or accidental destruction.

Verisk adheres to applicable laws, including the privacy and security regulations promulgated pursuant to the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (including the Health Information Technology for Economic and Clinical Health [HITECH] Act of 2009 and as updated via the Final Omnibus Rule of 2013) including any modifications of those acts.

Arrival and Acceptance

Data quality activities include field validity and field relationship edits; basic checks, such as balancing control totals; and additional checks, such as reasonability tests on aggregate data. In addition, the review process for aggregate data employs the judgment of actuaries and actuarial analysts familiar with insurance coverage and data as well as the external environment that can affect such data. The various data quality reviews help ensure the proper use and interpretation of the data in the downstream processing and development of information-driven products, such as loss costs.

While the ClaimSearch® team works closely with its member companies to help ensure data is processed and received correctly, it should be noted that the accuracy of the data maintained by ClaimSearch® is the sole responsibility of the submitting member company. Periodic audits and reviews are completed in coordination with members to help ensure data has been reported and represented appropriately from system to system.

Delivery of Data Products to External Entities

Production Services follows strict procedures in the delivery of products. IT Technology Operations validates that each customer is entitled to each product before product delivery.

Born from a dire need expressed by the insurance industry to combat the ever-growing increase of fraud, the goal of ClaimSearch® has been to act as the steward and custodian of member company data and assist with the open exchange of information between members as they investigate and handle claim activity. The exchange of data is completed through the ClaimSearch® application, and, in certain instances, system-to-system data feeds where relevant information is returned on a contributory basis.

D. Principal Service Commitments and System Requirements

Verisk Analytics, Inc. designs its processes and procedures to meet its objectives for its ClaimSearch® Platform. Those objectives are based on the service commitments that Verisk Analytics, Inc. makes to user entities, the laws and regulations that govern the provision of its ClaimSearch® Platform, and the operational, and compliance requirements that Verisk Analytics, Inc. has established for the services. The ClaimSearch® Platform of Verisk Analytics, Inc. is subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Verisk operates. Security, availability, processing integrity, confidentiality, and privacy commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security, availability, processing integrity, confidentiality, and privacy commitments are standardized and include, but are not limited to, the following:

- The use of security and confidentiality principles that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- The use of encryption technologies to protect customer data in transit over untrusted networks;
- The use of reasonable precautions to protect the security and confidentiality of the information that is collected;
- The use of availability principles that are designed to help ensure availability of the systems supporting the system;
- Make commercially reasonable efforts that controls are in place to automatically filter certain personal information collected from the System such as password and account numbers;
- Make commercially reasonable efforts that controls are in place to destroy or encrypt any information that is not filtered automatically;
- Make commercially reasonable efforts that controls are in place to help ensure complete and accurate processing of the in-scope system transactions; and
- Make commercially reasonable efforts to collect, use, retain, disclose, and dispose of personal information to achieve the Company’s service commitments and system requirements.

Verisk Analytics, Inc. establishes operational requirements that support the achievement of security, availability, processing integrity, confidentiality, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Verisk Analytics, Inc.'s system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data is protected.

E. Non-Applicable Trust Services Criteria

Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**Verisk Analytics, Inc.'s Rationale**
P 1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	N/A - The Company does not collect information directly from the Data Subject. The Member company is responsible for the collection of data from the Data Subject. Therefore, items such as communication of notice and consent to the Data Subject is not applicable.
P 2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	N/A - The Company does not collect information directly from the Data Subject. The Member company is responsible for the collection of data from the Data Subject. Therefore, items such as notice and consent to the Data Subject is not applicable.
P 3.1	Personal information is collected consistent with the entity's objectives related to privacy.	N/A - The Company does not collect information directly from the Data Subject. The Member company is responsible for the collection of data from the Data Subject. The Company's collection of data is subject to the privacy policies of Member companies. Therefore, this criterion is not applicable.

Security, Availability, Confidentiality, Processing Integrity, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**Verisk Analytics, Inc.'s Rationale**
P 3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	N/A - The Company does not collect information directly from the Data Subject. The Member company is responsible for the collection of data from the Data Subject. Therefore, items such as notice and consent to the Data Subject is not applicable.
P 4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	N/A - The Company does not collect information directly from the Data Subject. The Member company is responsible for the collection of data from the Data Subject. The Company's use of data is subject to its agreements with its Members. Therefore, this criterion is not applicable.
P 6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	N/A - The Company does not collect information directly from the Data Subject. The Member company is responsible for the collection of data from the Data Subject. Therefore, consent for disclosure to third parties from the Data Subject is not applicable.
P 7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	N/A - The Company does not collect information directly from the Data Subject. The Member company is responsible for the collection and accuracy of the data from the Data Subject. Therefore, this criterion is not applicable.

F. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
CyrusOne	Verisk uses multiple data centers for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Verisk's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Centers hosting the in-scope applications, and • Controls, including environmental controls, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes. In addition, the Company has identified the following controls to help monitor the subservice organization: • On a quarterly basis, physical access to the colocation data centers is reviewed by management to validate that employee access is appropriate based on job function, and • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and determines their risk rating based on their level of access, the sensitivity of the data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's system and organization control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	CC 6.4* A 1.2* A 1.3*
Amazon Web Services (AWS)	The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses various AWS Platform-as-a-Service components such as Amazon RDS and AWS Simple Storage Service (S3). The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform; • Controls over the configuration settings within the EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components (Amazon RDS and S3) such as physical servers and operating systems including applying critical patching for this infrastructure;	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4* CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over Amazon RDS and S3 including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls around AWS S3 redundancy, including controls over data replication; and • Controls around the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform (AWS RDS and S3) components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and determines their risk rating based on their level of access, the sensitivity of the data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's system and organization control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary, and • Backups for rapid onsite recovery of no less than four days are stored and assessed via active restorations of data to help ensure validity.	A 1.3* C 1.1* C 1.2* P 4.3* P 6.6* PI 1.4* PI 1.5*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.*

G. User Entity Controls

Verisk Analytics, Inc.'s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary user entity controls identified within the table below, where applicable. As applicable, suggested control considerations and/or complementary user entity controls and their associated criteria have been included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
User Entities (Member company) are required to train authorized users and inform them of the importance of the data and the necessity of securing that data.	CC 1.1 CC 1.2
User Entities (Member company) are required to inform their employees and agents of the nature and scope of their participation in ClaimSearch® Platform, along with all applicable laws, regulations, and other limitations.	CC 1.1 CC 1.2 P 8.1
User Entities (Member company) are responsible for notifying ClaimSearch® or deactivating the authorized user when authorized users have been terminated and for verifying that authorized users meet the requirements for access to the ClaimSearch® Platform.	CC 6.1* CC 6.2* CC 6.3*
User Entities (Member company) are responsible for performing background checks of their authorized users and ensuring that only qualified authorized users have access to the ClaimSearch® Platform.	CC 1.4* CC 6.1* CC 6.2* CC 6.3*
The User Entity (the NICB) is responsible for credentialing NICB participating organizations.	CC 1.4*
User Entities (Member company) are required to comply with credentialing procedures.	CC 1.4*
User Entities (Member company) are responsible for submitting accurate data to ClaimSearch®.	CC 2.3* PI 1.2* PI 1.3* PI 1.4* P 7.1*
User Entities (Member company) are responsible for authorizing users that can access claims information within their organization.	CC 6.1* CC 6.2* CC 6.3*
User Entities (Member company) are responsible for selecting and/or requesting data to be purged and/or destroyed in accordance with the User Entity's Data Destruction and Disposal Policy.	CC 6.5* C 1.1* C 1.2* P 4.2* P 4.3* PI 1.5*
User Entities (Member company) are responsible for implementing a follow up process for responding to rejected files and correcting any issues associated with the data input process (SFTP and XML processes).	PI 1.2* PI 1.3* PI 1.4*

User Entity Control	Associated Criteria
User Entities (Member company) are responsible for the collection of data from the Data Subject. Therefore, items such as communication of notice and consent is the responsibility of the Member Company.	P 1.1 P 2.1 P 3.1 P 3.2 P 4.1 P 6.1 P 7.1
User Entities (Member company) are responsible for requesting to delete, update, and/or modify personal information from its database.	P 4.3* P 5.2* P 6.7* P 7.1 P 8.1*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary user entity controls that support the service organization's service commitments and system requirements are in place and are operating effectively.*

Aprio