Verisk™

Verisk’s Approach to Cybersecurity

Version 1.3

May 2024

Table of Contents

Introduction

As a leading data analytics and technology partner to the global insurance industry, we know that data is the lifeblood of our organization and protecting that data is paramount.

As Verisk continues to grow and expand with respect to the markets we serve, the geographies we operate in, and the scope of solutions and related technologies we provide to our clients, we are keenly aware of increased exposure to potential risk and remain steadfast in our commitment to safeguarding the integrity, confidentiality, and responsible use of data.

It’s Verisk’s vision to be the world’s most effective and responsible data analytics company in pursuit of our customers’ most strategic opportunities. To that end, Verisk has made a dedicated commitment to:

- building a culture that is both strongly aware of the critical need to protect the confidentiality of data collected and ever vigilant in execution of safeguards to protect the data;
- investing in strong internal governance processes that include dedicated information risk officers, investment in security improvements, mandatory employee security training, and diligence of third-party vendors;
- complying with all applicable legal requirements and regulations;
- building and maintaining trust and transparency with regulators, clients, and consumers; and acting ethically and responsibly

This document provides an overview of Verisk’s comprehensive and rigorous approach to cybersecurity designed to keep the data entrusted to us safe. It is for informational purposes only and does not constitute any binding agreement nor establish any legally enforceable obligation. It is subject to modification at the sole discretion of Verisk. If there is a conflict between this overview and any formal corporate policy, guideline, or other governing document (“controlling requirement”), the controlling requirement shall apply and govern.

Cyber Risk Governance

Verisk’s approach to enterprise cyber risk governance, as depicted in the illustration below, is designed to fulfill the company’s data responsibility objectives throughout all facets of the company.

<table>
<tr><th colspan="4">Board of Directors</th></tr>
<tr><th colspan="3">Executive Risk Management Committee</th><th>Audit Function</th></tr>
<tr><th colspan="2">Enterprise Risk Management</th><th colspan="2">Verisk Businesses and Corporate Functions</th></tr>
<tr><td>Cybersecurity</td><td>Cyber Insurance and Insurance Management</td><td>Security Awareness and Training</td><td>Risk Identification</td></tr>
<tr><td>Personnel Security and Business Continuity</td><td>Third Party Risk</td><td>Security and Compliance Councils</td><td>Risk Assessment</td></tr>
<tr><td>GRC / Risk Systems</td><td>Corporate Credentialing</td><td>Service Delivery</td><td>Risk Treatment</td></tr>
<tr><th colspan="2">Policy and Oversight</th><th colspan="2">Data Protection</th></tr>
</table>

The program is founded on direction and priorities established by Verisk’s leadership, supported and overseen by the Board of Directors, and deployed through an enterprise risk management framework (Framework). The Framework leverages proven standards such as those embedded in the NIST Cybersecurity Framework (CSF), which is generally accepted by leaders in financial services industry, the federal government, and cybersecurity leaders.

Board of Directors Oversight

Verisk’s Board of Directors oversees the company's management of cybersecurity, including oversight of appropriate risk mitigation strategies, systems, processes, and controls. The Board of Directors receives regular reports from executives about the company’s cybersecurity risks, management review processes, overall health, and readiness to respond to an incident.

Cyber Risk Management Leadership Roles

The Executive Risk Management Committee (ERMC), which includes the top corporate executives, provides guidance and authority related to the enforcement of Verisk’s Framework, including the strategies, policies, procedures, processes, and systems, established by management to identify, assess, measure, monitor, and manage risks. The ERMC also reinforces the corporate risk appetite and determines whether residual risk is acceptable.

The Enterprise Risk Management (ERM) division oversees and advises on implementation of the Framework throughout the Verisk businesses. In doing so, the ERM division aggregates and assesses risk across the enterprise. Within the division are Verisk’s Cybersecurity and Information Risk Management functions that partner with the Verisk businesses to help ensure that risk management strategies are implemented. In collaboration with other Verisk divisions, the ERM division contributes to training and awareness processes, sponsors working groups across the enterprise on critical security topics and provides centralized incident response.

Ownership and Accountability of Each Verisk Business

Verisk businesses have dedicated liaisons assigned for risk management activities, who participate in a global security council designed to facilitate implementation of the Framework and associated policies. As custodians and/or processors of our stakeholders' data, Verisk businesses also accept certain compliance responsibilities, including but not limited to, security obligations pursuant to the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Gramm-Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Payment Card Industry Data Security Standard (PCI DSS), all to the extent applicable. For each of its businesses, Verisk seeks to actively confirm that its security risk management practices fulfill applicable legal, contractual or other requirements.

Promoting a Culture of Awareness and Ownership with All Associates

Verisk recognizes that all Verisk employees and many third parties have significant roles and responsibilities in ensuring the fulfillment of Verisk's risk management strategy and objectives. In summary, these roles and their responsibilities include:

- The Verisk workforce (employees and third parties) is accountable for understanding and complying with all security policies, guidelines, and procedures, including Verisk's Acceptable Use Policy that establishes the responsibilities for the workforce when using company assets.
- Internally designated data owners report to and are empowered by the executive management of their respective Verisk business and have full accountability for the security of the business unit's segment of products and services.
- Application owners are responsible for the overall procurement, development, integration, modification, and operation and maintenance of application systems supporting Verisk businesses and functional units.
- Systems owners are responsible for providing the technology services for the set of application systems and related infrastructure supporting Verisk businesses.

Policies and Governing Documents

Policies governing our operations are written and designed to embed industry leading controls to help mitigate risk to our Verisk businesses and related data. Policy implementation is achieved by applying three lines of defense, whereby: 1) our Verisk businesses implement controls to maintain policy compliance and facilitate data protection, 2) our Enterprise Risk Management functions collaborate with our Verisk businesses to manage cyber risk, and 3) our system is audited by both internal and external auditors to assess adherence to our policies and industry best practices.

Executive management authorizes a risk policy, an information security framework document, and supporting policies that support our comprehensive cyber risk culture. The risk policy defines what risk means to our Verisk businesses, as well as the enterprise risk management framework and governance model described in this document.

The information security policy framework defines the fundamental principles for the protection of enterprise-wide information resources, the proper controls needed to ensure compliance with applicable legal requirements and internal policies; and serves to uphold Verisk's reputation with our clients. Verisk employees, contractors, and third parties are responsible for complying with information security policies.

External Audits, Certifications, and Attestations

Verisk's control environment, including controls related to cybersecurity described in this document, are regularly subject to independent testing from both internal and external audits. A closed-loop corrective action process manages any potential exceptions identified during audits.

AICPA Service Organization Control (SOC) 2 Report

Verisk's corporate-managed security services have successfully taken part in annual Service Organization Control (SOC 2 type II) attestation examinations each year since 2011. The examination process includes a detailed description and independent attestation and testing of the controls and services adopted by Verisk management. This attestation is performed in accordance with the trust services principles of the AICPA (Association of International Certified Professional Accountants) covering security, privacy, confidentiality, integrity, and availability.

ISO 27001 Certification

Verisk's corporate-managed security services operate within an Information Security Management System (ISMS) in accordance with ISO 27001standards. The ISMS is an overarching management framework through which the organization identifies, analyzes, and addresses its information risks. The ISMS ensures that the security program is fine-tuned to keep pace with evolving security threats, vulnerabilities, and business impacts. Certification of compliance with this standard requires successful completion of a formal audit by an independent and accredited certification body.

International Data Transfers

Verisk complies with all laws, conventions, and guidelines governing international data transfers. Verisk business units have adopted appropriate policies, procedures, contracts, and security measures to ensure that data transferred from international locations to the United States meets government and client expectations.

Risk Identification and Management

Risk Assessment

Verisk's process for risk management aligns with enterprise strategic objectives and defines expectations for the organization to identify, assess, and manage risk. Verisk conducts various risk assessments with our businesses no less than annually to understand cybersecurity risk to organizational operations. Results from risk assessments serve two primary purposes: first, the results inform Verisk's cyber risk management strategy, objectives, and key initiatives; and second, if any material risks are identified, they require risk response and action plans to mitigate identified risks.

The risk response process requires identification of the particular business owner and affected process owners. The Information Risk Management team oversees plans for control activities to implement risk responses and to identify costs, benefits, and execution responsibilities of control and process owners.

Asset Management

Verisk has an established asset management policy and associated procedures to ensure the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and Verisk's risk strategy. The policy includes assets managed on premises as well as those supported by third-party hosting and cloud-based services.

Supply Chain Risk Management

Verisk has established a third-party risk management policy and supporting processes to identify, assess and manage supply chain risk. The policy requires that vendors are assessed and tiered based on their risk to the company. Vendors are then subjected to varying levels of due diligence and ongoing monitoring that aligns with the inherent risk of services they provide. Suppliers are required to acknowledge and commit to compliance with a Supplier Code of Conduct.

Risk Prevention and Protection

To provide for the security and resiliency of its systems and assets, Verisk has deployed a defense-in-depth strategy of protective solutions.

Identity Management and Access Control

Verisk has established policies, procedures, and associated system functionality to 1) limit access to physical and logical assets and associated facilities to authorized users, processes, and devices, and 2) manage access consistent with the assessed risk of unauthorized access. Information access is governed by the principle of least privilege, where access is limited to that which is necessary to perform job responsibilities.

Customer Credentialing Process

The Verisk Corporate Credentialing Policy requires the credentialing of outside parties that receive data products and services containing personally identifiable information (PII) to ensure the information accessed and its use is limited to authorized users and purposes. This process is subject to regular internal audits, with reporting to executive management and the Board of Directors.

Physical Security

Verisk has deployed policies, procedures, and supporting systems so each facility where customer data is processed or stored, have appropriate physical access controls in place to protect it from unauthorized access. Controls include, but are not limited to, physical access management systems and badges, CCTV monitoring, secure disposal of information, and process to ensure only authorized visitors enter Verisk facilities.

Data Protection

Verisk has deployed policies and controls to provide assurance that information and records (data) are managed consistent with the company’s risk strategy and governing data principles to protect the confidentiality, integrity, and availability of the data. Verisk classifies data based on the sensitivity of the information. Specific handling and data security controls are defined and deployed depending on data classification. Available controls include, but are not limited to, authorization, encryption, tokenization, and secure disposal or destruction.

Application and Infrastructure Security

Verisk has deployed security policies that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, as well as processes and procedures that are maintained and used to manage the protection of information systems and assets.

Perimeter Security

Verisk has deployed security policies that require controls to maintain the security of Verisk's network and email perimeter. Vulnerability assessments are proactively performed so Verisk can continuously monitor and enhance its defenses.

Secure Development and Change Management

Verisk has deployed a secure development policy and related procedures, which are designed to provide assurance that secure coding practices are infused throughout Verisk's system development life cycle (SDLC), and to uphold data quality standards and practices, from initial planning through disposal of the system.

Configuration Management

Verisk has deployed policies and related procedures that are designed for consistent and secure configuration baselines across the Verisk enterprise to encompass relevant components such as endpoints (laptops, desktops, browsers, and mobile devices), operating systems, application services, virtualization, and cloud services.

Endpoint Security

Verisk has deployed policies and procedures to manage endpoints and to identify and protect against malicious or suspicious activity. Verisk patches endpoints to reduce the likelihood of a vulnerability being exploited, and there are internal processes to authorize the use of removable media.

Awareness and Training

Verisk provides its workforce, including personnel and partners, cybersecurity awareness education and training to enable them to perform their information security-related duties and responsibilities consistent with Verisk policies, procedures, and agreements. In addition, Verisk conducts unannounced enterprise phishing assessments targeting our workforce, with additional training enrollments for individuals that fail the assessment.

Monitoring and Detection

Continuous Monitoring

Verisk establishes logging and monitoring capabilities to enable the ongoing review of user activities and timely detection of potential vulnerabilities, malicious or suspicious activity, potential security violations, performance, and processing exceptions. Verisk's Security Operations Center (SOC) operates on a 24/7/365 basis to monitor, identify, respond to, and remediate any incidents that threaten the confidentiality, integrity, and availability of Verisk's information systems. The SOC leverages data from Verisk information technology and security components, authentication platforms, threat intelligence feeds, as well as other sources.

Response and Recovery Planning

Incident Response Program (IRP)

Verisk's ERM organization has established an IRP that includes policies and procedures that encompass the life cycle of incident management. Verisk employs highly skilled cyber professionals and has defined roles and responsibilities in detail for each stage of the IRP, as outlined below.

IRP phase	Key activities
Preparation	Incident response procedures are defined in detailed for potential scenarios. Communications and coordination procedures are defined in detail. Plans are communicated and periodically tested.
Identification	Incidents are assessed and classified according to Incident Classification criteria defined in the Verisk incident response plan. The appropriate teams are activated and investigate the incident including collecting evidence and performing root-cause analysis.
Containment	Approaches are defined and deployed to limit the impact of the incident. This includes limiting the incident to affected assets and providing notification in accordance with applicable laws and contractual obligations.
Eradication	The root cause of the incident is identified. As appropriate, affected systems are removed from the environment or taken offline.
Recovery	Affected systems and devices are restored and returned to the business environment in a manner that ensures no threat remains.
Lessons Learned	Analysis is performed to ultimately learn from incident and potentially improve future response efforts and incident documentation is completed.

Business Continuity Program (BCP)

Verisk has established a BCP consisting of policy and supporting procedures to protect the safety of Verisk personnel, guests, and business partners, and to enable the timely recovery of services and information systems to conform to business management, regulatory, and customer requirements. BCP components include:

- Crisis management plans
- Emergency response plans
- Risk and vulnerability assessments
- Business impact analysis
- Business continuity planning
- Pandemic plans

Data Backup

All Verisk businesses and functional areas manage data backup strategies in accordance with their business requirements and within requirements of any applicable laws and regulations.