Verisk's Approach to Cybersecurity

Version 1.1
November 2020

Contents

Introduction

As a leading data analytics provider, we know that data is the lifeblood of our organization and protecting that data is of paramount importance.

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 customers, 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 compliance officers and 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, customers, and consumers; and
- acting 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 and Compliance</th><th colspan="2">Verisk Business</th></tr>
<tr><td>Cybersecurity</td><td>Compliance and Privacy</td><td>Security and Compliance Councils</td><td>Risk Identification</td></tr>
<tr><td>Information Risk</td><td>Third Party Risk</td><td>Awareness and Training</td><td>Risk Assessment</td></tr>
<tr><td>Personnel Security and Business Continuity</td><td>Cyber Insurance</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 are 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 and Compliance (ER&C) division oversees and advises on implementation of the Framework throughout the Verisk businesses. In doing so, the ER&C 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. The ER&C division also hosts training and awareness sessions, 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, aspects of 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 (PCI) standard, all to the extent applicable. For each of its businesses, Verisk seeks to actively confirm that its risk management practices fulfill applicable compliance 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 designed to 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 and Compliance functions integrate 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 uphold Verisk's reputation with our clients. Verisk employees, contractors, and third parties are responsible for ensuring compliance with all 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

The Verisk regional data centers 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 27001:2013 Certification

Verisk has implemented an Information Security Management System (ISMS) in accordance with ISO 27001:2013 standards. 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 are Privacy Shield–certified and 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.

- Information assets are clearly identified, documented, and regularly updated in a centrally managed inventory, which includes designated business, data, application, and system owners.
- Verisk classifies data based on the value and sensitivity of the information to the organization. Specific handling and data security controls are defined and deployed depending on data classification.
- Software installed on any machine connecting to a Verisk or member company network must be used only for authorized business purposes.

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, which includes privacy and confidentiality provisions.

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, including the following:

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. These controls include but are not limited to:

- Access requests initiated by a member of Verisk's workforce are associated with a corresponding "common identifier" (a user ID) that serves as an element of authentication and is designed to provide both nonrepudiation and audit logging.
- Information access is governed by the principle of least privilege, where information access is limited to that which is necessary to perform job responsibilities.
- Access to Verisk information is controlled through a managed process that addresses authorizing, modifying, and revoking access, as well as a periodic review of information system privileges.
- Web filtering functionality is deployed to manage Internet access. Internet search or access requests are routed through the filter, which blocks access to inappropriate or potentially harmful websites and otherwise enforces corporate and regulatory policy compliance.
- Remote access to Verisk information assets is controlled through multi-factor authentication.
- Vendor access to any information assets is governed by associated data classification handling requirements.

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 of its facilities, including data centers and storage facilities, have appropriate physical access controls in place to protect it from unauthorized access. Those controls include but are not limited to the following:

- Physical access management systems are deployed for Verisk facilities, including data centers and storage facilities.
- CCTV monitoring on a 24/7 basis is often deployed at points of access to Verisk facilities and within Verisk controlled secure spaces, including those with high concentrations of sensitive data.
- Physical and printed media and other types of physical assets are disposed of by confidential means, such as shredding or confidential disposal services.
- Visitors to Verisk facilities must present a valid government ID and be escorted by a Verisk employee.

Data Protection

Verisk has deployed 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. These controls include but are not limited to the following:

- Data is classified according to a data classification and handling policy.
- Data is controlled and managed in accordance with the data handling requirements set forth in the policy, which considers our Verisk global workforce, compliance requirements for offshore access, and customer requirements for data sharing and segregation.
- Sensitive data is restricted to only authorized individuals, and such data is protected (i.e. tokenized, encrypted, etc.) in accordance with industry best practice methods when stored or processed.
- Non-publicly available data is encrypted by industry-leading protocols and algorithms when in transit or at rest.
- Data is encrypted on any mobile device that has the capability to store Verisk information, including mobile devices, laptops, notebooks, and smartphones.
- Data is encrypted on any media used for purposes of disaster recovery, business continuity, and archiving.
- Data storage is encrypted for any remotely accessible Verisk information assets, including but not limited to web-accessible resources and file-sharing systems.
- Development and testing environments are separated from production environments.
- Data is retained in accordance with our global records management policy, in alignment with business need, and per applicable laws and regulations.
- Verisk generally follows industry standards for data disposition and destruction that involves methods specific to the media or storage type, so information cannot be retrieved or reconstructed in the event the storage device is either reused or destroyed.

Application and Infrastructure Security

Verisk has established 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's network is architected to restrict access to only authorized users for authorized services for both external and internal parties.
  - Multiple firewall devices at external access points into the network prevent intrusion, limit accessible services, and isolate Verisk's network from those of customers and other third parties.
  - Firewalls protect Internet-facing infrastructure and applications. There are firewalls between demarcation zones and Verisk's internal network.
  - Firewalls restrict access between network segments to allow only authorized personnel access to specifically configured services.
- Web application firewalls are deployed to protect web applications from malicious activities such as cross-site request forgery, cross-site scripting (XSS), and SQL injection.
- Secure e-mail gateway services supported by dynamically updated threat intelligence feeds are deployed to evaluate inbound e-mail traffic, blocking or quarantining e-mails exhibiting suspicious characteristics. Examples of these controls are reputation filters for known malicious senders or those that spoof otherwise trusted senders, content filters for spam or malware, and threat filters for phishing or other non-malware based social engineering threats such as business e-mail compromise attempts.

- Vulnerability and penetration assessments are proactively performed to simulate an external attacker, so Verisk can enhance its defenses, with findings remediated within internally defined service level agreements.

Secure Development and Change Management

Verisk has developed and published 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. Significant development requirements include but are not limited to:

- Development adheres to secure standards set forth by the Open Web Application Security Project (OWASP) and the Application Security Working group (ASWG).
- Development staff are trained in current secure coding practices.
- Verisk member companies follow a SDLC process that undergoes reviews by Verisk's Enterprise Risk and Compliance division.
- Production code is reviewed using security checkpoints throughout the system development life cycle to enable consistent application of security.
- Changes follow a formal change control procedure to enable the security and integrity of the information and information system.
- Static code scanning and/or dynamic code scanning is performed for systems, and systems must be void of any known vulnerabilities rated as high or critical prior to release to production.

Configuration Management

Verisk's configuration management policy and related procedures are designed to ensure that consistent and secure configuration baselines are established and maintained 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. Specific controls include but are not limited to:

- Maintaining baseline configurations as current, using automated mechanisms to reflect approved changes.
- Following a formal change control process that includes oversight from a change advisory board.
- Automating change control process, and other mechanisms, such as file integrity monitoring, to detect and prevent unauthorized changes.
- Enforcing access restrictions, logging, and log review of changes to confirm changes are properly approved.
- Deploying automated mechanisms to verify correct operation of security functions upon system startup and restart and to provide notification and alerts of failed security tests.
- Scanning cloud-based environments weekly to identify any configuration changes not consistent with baseline configuration standards and security rules.

Endpoint Security

Verisk has enacted policies and procedures to manage endpoints, prevent vulnerabilities whenever feasible, and otherwise identify and promptly remediate the occurrence of vulnerabilities. These include but are not limited to:

- Verisk patch management program is based on best practices, including maintaining a current inventory of IT components, risk rating these components for patch relevancy, monitoring vendor patches, establishing a patch deployment schedule based on applicability and risk rating, and following a controlled change management process for patch deployment, testing, and release to production.

- Endpoint detection and response software is installed on endpoints to prevent malware and provide forensic capability to assist with incident response.
- Antivirus/antimalware software is installed on Verisk endpoints, and employees are prohibited from disabling such software.
- Endpoint data loss prevention software is installed on endpoints that restricts use of removable media.

Awareness and Training

Verisk provides the members of 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.

- Employees must acknowledge and adhere to key Verisk information security policies upon hiring and on a regular basis thereafter.
- Employees also receive information security training tailored to specific job functions upon hiring and thereafter on a regular basis.
- Employees with elevated system privileges and those with information security responsibilities receive a more intense level of training relative to their specific functions.
- 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 and reconstruction of user activities and timely detection of potential vulnerabilities, malicious activity, security violations, performance, and processing exceptions.

- User-related audit logs are maintained for a wide range of system activities and regularly reviewed for indications of anomalous activities. Activities that are logged and monitored include but are not limited to successful and unsuccessful login attempts; actions performed by privileged users; changes, additions, or deletions to any account with root or administrative privileges; and the creation, deletion, and modification of system-level objects. Logs maintained by Verisk are attributable to a unique user, and time synchronization technology is leveraged to assist with the maintenance of an accurate audit trail.
- System components and applications are configured such that audit logs, network telemetry data (e.g., packet metadata), and security events from across the enterprise are captured in a centralized Security Incident and Event Monitoring (SIEM) system.
- Verisk performs frequent scans to monitor for potential vulnerabilities to applications, networks, operating systems, and cloud services. Those potential vulnerabilities are assigned severity ratings that determine the required remediation timeframe.
- Database activity monitoring is employed for critical database systems with regular review for suspicious or anomalous activity.
- Data loss prevention (DLP) software is deployed to monitor potential data exfiltration and generate triggers for incident management purposes and provide logging for forensic purposes.
- Verisk User and Entity Behavioral Analytics (UEBA) incorporates machine learning to enhance user and peer group behavioral analysis. Machine learning enables risk scoring to be applied to potential anomalies that reflect the likelihood of a threat related to the anomalous behavior. Verisk UEBA automatically triggers and prioritizes incident response events.

- Verisk 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 security components such as firewalls, intrusion protection systems, and authentication platforms, as well as other sources.

Response and Recovery Planning

Incident Response Program (IRP)

Verisk has established an IRP that includes policies and procedures that encompass the life cycle of incident management. Verisk has defined roles and responsibilities in detail for each stage of the IRP, as outlined below. Personnel must successfully complete training before being assigned IRP responsibilities and at least annually thereafter.

Verisk's ER&C organization oversees IRP planning, deployment, and execution for the entire IRP life cycle.

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 policy. 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 hosts and 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 production environment, any malware is securely removed, systems are hardened and patched, and updates are applied.
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 create and manage a data backup plan to fulfill BCP and disaster recovery requirements in accordance with the Verisk Business Continuity Management Policy and applicable laws and regulations.