Version 2.0 | August 2026
Prepared for public corporate responsibility disclosure

Verisk's Approach to Cybersecurity

A risk-based approach to protecting data, technology, people, and operations



Verisk remains steadfast in our commitment to safeguarding the confidentiality, integrity, availability, and responsible use of data.

IMPORTANT NOTICE

This document provides a high-level overview of Verisk's approach to cybersecurity risk management and governance. It is for informational purposes only, does not constitute a binding agreement, and does not establish a legally enforceable obligation. Practices may vary by business, service, system, location, risk, and applicable requirement. If this overview conflicts with a formal Verisk policy, standard, procedure, contract, or other governing document, the governing document controls.

Table of Contents

1. Our commitment 3
Cybersecurity principles 3
2. Cybersecurity governance 3
Board and management oversight 3
Shared accountability 4
Policies and governing documents 4
3. Identify: risk, assets, and third parties 5
Cybersecurity risk management 5
Asset and data management 5
Third-party and supply chain risk 5
4. Protect: people, data, technology, and facilities 6
Identity and access management 6
Data protection and stewardship 6
Application, cloud, and infrastructure security 6
Artificial intelligence security 6
People and physical security 7
5. Detect: monitoring and security operations 7
6. Respond: incident management 8
7. Recover: resilience and continuity 8
8. Assurance, certifications, and continuous improvement 9
Independent assurance 9
Certifications and attestations 9
Continuous improvement 9
9. Scope and important qualifications 9

1. Our commitment

As a vital partner to the global insurance industry, Verisk knows that building resilience is a team effort. Data, analytics, technology, and deep industry knowledge are central to the value we deliver. Protecting the data and systems entrusted to us is therefore fundamental to our ability to serve clients and support stronger, more resilient businesses and communities.

Verisk's cybersecurity program is designed to safeguard the confidentiality, integrity, availability, and responsible use of data. The program combines governance, risk management, preventive and detective controls, incident response, recovery planning, independent assurance, and continuous improvement.

Our approach is risk-based and informed by recognized standards, including the National Institute of Standards and Technology Cybersecurity Framework. It is integrated with enterprise risk management and applies across Verisk, with implementation calibrated to business context, data sensitivity, technology architecture, legal and contractual requirements, and the services being provided.

Cybersecurity principles

- Accountability: leaders, business owners, system owners, data owners, and the workforce share responsibility for managing cybersecurity risk.
- Risk-based protection: controls are selected and prioritized based on threats, vulnerabilities, business criticality, and the sensitivity of data and systems.
- Defense in depth: organizational, technical, physical, and procedural safeguards work together to reduce the likelihood and potential impact of security events.
- Resilience: cybersecurity includes preparation to maintain or restore critical services following disruption.
- Continuous improvement: risk assessments, testing, monitoring, incidents, changes in technology, and lessons learned inform program improvement.

2. Cybersecurity governance

Cybersecurity governance establishes direction, accountability, decision rights, oversight, and reporting. Verisk's governance model connects Board oversight, executive management, security leadership, business ownership, independent assurance, and workforce responsibilities.

Board and management oversight

The Board of Directors oversees Verisk's management of cybersecurity risk, including risk mitigation strategies and readiness to respond to incidents. The Board's Risk Committee oversees risk assessment and risk management in coordination with other relevant Board committees, including Verisk's policies, procedures, and strategic approach to cyber, technology, and information security risk. Management

provides the Board Risk Committee with regular updates on cybersecurity developments, material risks, and mitigation strategies.

The Executive Risk Management Committee provides management guidance and authority for the enterprise risk framework, including cybersecurity strategies, policies, processes, systems, risk appetite, and significant risk treatment decisions.

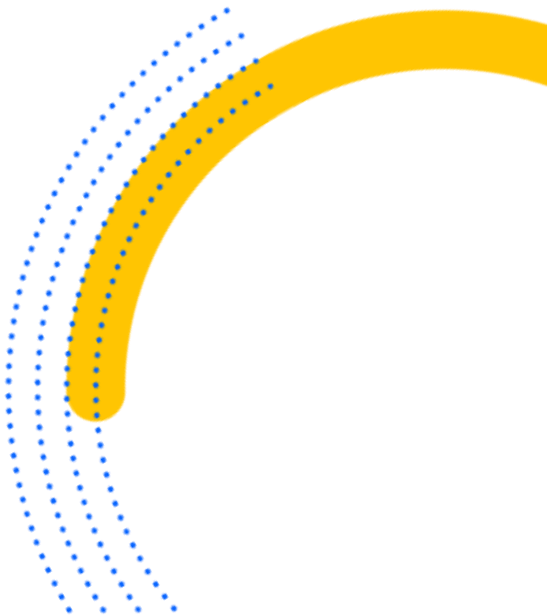
Enterprise Security leads the cybersecurity program, partners with business and functional teams, aggregates and assesses risk, and coordinates security operations and incident response.

Shared accountability

- Business and functional leaders are accountable for managing cybersecurity risks within their operations and for implementing applicable requirements.
- Data, application, and system owners define and maintain protections appropriate to the information and technology under their responsibility.
- Information risk and security professionals advise the business, perform or review assessments, monitor risk treatment, and support governance reporting.
- The workforce is responsible for following security requirements, protecting Verisk information and technology, and promptly reporting suspected incidents or unsafe conditions.
- Internal Audit and external assessors provide independent assurance within their respective scopes.

Policies and governing documents

Verisk maintains an enterprise information security policy framework supported by standards, procedures, and other governing documents. These requirements address topics such as risk management, identity and access, data classification and handling, secure development, vulnerability management, logging and monitoring, incident response, third-party risk, physical security, business continuity, and acceptable use. Requirements are reviewed and updated as the risk, technology, business, and regulatory environment evolves.



3. Identify: risk, assets, and third parties

Cybersecurity risk management

Verisk identifies and evaluates cybersecurity risks through enterprise and business-level processes. Risk assessments consider threats, vulnerabilities, existing controls, business impact, data sensitivity, technology dependencies, third parties, and applicable obligations. Results inform priorities, investment decisions, remediation plans, risk acceptance, and governance reporting.

Risk treatment may include reducing risk through additional controls, avoiding an activity, transferring risk, or accepting residual risk through an authorized process. Accountable owners and target actions are identified, and progress is monitored based on risk.

Asset and data management

Verisk maintains processes to identify and manage technology assets, information assets, cloud services, software, and supporting dependencies. Ownership and classification help determine protection, monitoring, retention, and recovery requirements. Asset information is maintained and updated through risk-based processes that support operational and security decision-making.

Third-party and supply chain risk

Verisk maintains a third-party risk management program to identify, assess, and manage cybersecurity risks associated with suppliers and other external dependencies. The depth and frequency of due diligence and monitoring are based on factors such as data access, connectivity, service criticality, technology dependency, and the potential business impact of disruption or compromise.

- Security, privacy, confidentiality, incident notification, business continuity, and assurance expectations may be addressed in due diligence, supplier requirements, and contractual terms, as appropriate.
- Supplier access is limited to authorized purposes and is removed when no longer required.
- Higher-risk relationships may receive enhanced review, monitoring, testing, or recovery coordination.
- Material changes, incidents, and control concerns may trigger reassessment or additional risk treatment.



4. Protect: people, data, technology, and facilities

Verisk uses layered safeguards intended to reduce the likelihood and impact of unauthorized access, misuse, loss of data, and disruption. The design and operation of controls vary according to risk, service scope, system architecture, and applicable requirements.

Identity and access management

- Access is based on business need, role, risk, and least-privilege principles.
- User identities and access rights are managed through authorization, provisioning, review, modification, and removal processes.
- Stronger authentication and privileged access protections are applied based on risk and system requirements.
- Access activity is logged and monitored where appropriate to support accountability, investigation, and auditability.

Data protection and stewardship

Verisk's approach to data stewardship includes protecting the security and privacy of data through governance, policies, standards, technology, training, and third-party oversight. Data is classified and handled according to sensitivity, use, and applicable requirements. Protective measures may include access controls, encryption, segregation, tokenization or masking, data loss prevention, retention controls, and secure disposal.

Cybersecurity supports responsible data use by protecting information from unauthorized access, alteration, disclosure, or destruction. Privacy, compliance, and data governance teams maintain complementary requirements and processes within their respective areas of responsibility.

Application, cloud, and infrastructure security

- Security is integrated into technology architecture, system development, acquisition, deployment, change, and maintenance processes.
- Secure development practices may include threat modeling, secure coding guidance, code review, automated scanning, dependency analysis, security testing, and risk-based remediation.
- Technology configurations are managed against approved standards, with monitoring for unauthorized or risky changes where appropriate.
- Network, email, web, endpoint, and cloud security controls are used to reduce exposure to malicious activity and unauthorized access.
- Vulnerability management uses discovery, assessment, prioritization, remediation, and validation processes informed by severity, exploitability, exposure, and business impact.

Artificial intelligence security

Verisk applies cybersecurity and risk management principles to the use and development of artificial intelligence. Security considerations may include authorized use, data protection, access control, model

and application risk, third-party dependencies, secure development, testing, monitoring, and incident response. These activities complement Verisk's broader commitment to ethical and responsible AI, including human-centered values, fairness, transparency, and governance.

People and physical security

Verisk provides cybersecurity awareness education and role-appropriate training so personnel can understand their responsibilities, recognize threats, and report suspected incidents. Awareness activities may include phishing simulations, targeted communications, and additional training based on role or risk.

Physical security measures protect people, facilities, systems, and information. Controls may include access management, visitor processes, monitoring, secure areas, and secure disposal. For hosted, colocation, and cloud environments, relevant physical and environmental controls may be operated by service providers and assessed through contractual, due diligence, and assurance processes.

5. Detect: monitoring and security operations

Verisk maintains logging, monitoring, analysis, and security operations capabilities to identify suspicious activity, vulnerabilities, control weaknesses, and potential cybersecurity incidents. Monitoring is risk-based and may be performed through enterprise capabilities, business-specific capabilities, or qualified service providers.

- Security events and relevant telemetry are collected and analyzed to support detection, triage, investigation, and response.
- Vulnerability and configuration monitoring help identify weaknesses and deviations from approved security expectations.
- Threat intelligence and external monitoring inform situational awareness and defensive priorities.
- Data protection monitoring may help identify potential unauthorized access or transfer.
- Detection processes are reviewed and tuned as systems, threats, and business needs change.

6. Respond: incident management

Verisk maintains an incident response program with defined roles, escalation paths, communications, investigation, containment, eradication, recovery, and post-incident improvement activities. The program coordinates security, technology, legal, privacy, communications, business, and other specialists based on the nature and severity of an event.

Phase	Core activities
Prepare	Maintain plans, playbooks, roles, communications, tools, training, exercises, and external support arrangements.
Identify	Triage and classify events, investigate scope and impact, preserve relevant evidence, and activate appropriate teams.
Contain	Limit impact, isolate affected assets or services, protect critical operations, and coordinate required decisions and notifications.
Eradicate	Address root causes, remove malicious artifacts, remediate vulnerabilities, and strengthen affected environments.
Recover	Restore services in a controlled manner, validate security and operational readiness, and monitor for recurrence.
Improve	Complete post-incident reviews, track corrective actions, and incorporate lessons into controls, plans, training, and governance.

7. Recover: resilience and continuity

Verisk maintains business continuity and disaster recovery practices intended to sustain or restore critical services after disruptive events. Business impact analysis, continuity planning, technology recovery, crisis management, emergency response, testing, and improvement activities are performed according to business and service requirements.

Recovery strategies consider the criticality of services, technology and supplier dependencies, recovery objectives, data protection, geographic and cloud architecture, and applicable obligations. Backup and restoration capabilities are designed and managed according to risk and recovery requirements. Critical suppliers may be included in continuity planning, testing, and recovery coordination.

8. Assurance, certifications, and continuous improvement

Independent assurance

Verisk's control environment is evaluated through a combination of management review, internal audit, external audit, independent assessments, penetration testing, and other assurance activities. Findings are evaluated and tracked through corrective action or risk treatment processes. The availability of reports may be subject to confidentiality, contractual, and security requirements.

Certifications and attestations

Verisk maintains recognized certifications and attestations for defined in-scope services and control environments. These may include ISO/IEC 27001:2022 certification for core enterprise security services which includes ISO/IEC 27017:2015 certification for applicable cloud security controls, and SOC 2 Type II examinations for relevant services. Certification and report scope, period, criteria, and exclusions are defined in the applicable certificate or assurance report.

Continuous improvement

Verisk uses risk assessments, metrics, control testing, audit results, threat intelligence, incident lessons, technology changes, business priorities, and stakeholder feedback to improve the cybersecurity program. Improvement priorities are governed and tracked according to risk, accountability, and resource considerations.

9. Scope and important qualifications

- This document is a general overview. It is not a control catalog, security addendum, certification, warranty, or representation that any particular control applies uniformly to every product, system, location, service, or third party.
- Cybersecurity practices evolve. Verisk may modify its program, controls, organizational structure, technologies, and service providers based on risk, business needs, and applicable requirements.
- Specific security commitments are governed by applicable contracts, policies, standards, procedures, assurance reports, and certificates.
- No cybersecurity program can prevent or detect every threat or incident. Verisk uses risk-based measures intended to manage cybersecurity risk and support resilience.
- Questions about a specific service, certification scope, control, or assurance report should be addressed through the applicable Verisk client or third-party risk management process.