THOMSON REUTERS®

Thomson Reuters Information Security Principles

March 2023

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting, and compliance professionals combined with the world's most global news service – Reuters. For more information on Thomson Reuters, visit tr.com and for the latest world news, reuters.com.

We maintain our reputation for providing reliable and trustworthy information through a variety of means, including a comprehensive information security management framework supported by a wide range of security policies, standards, and practices.

This document explains Thomson Reuters' approach to information security and risk management.

White Paper

Contents

Thomson Reuters operates a global information security organization that is aligned with the NIST CSF.

Information Security Strategy Overview

Thomson Reuters operates a global information security organization aligned with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). We strive to continuously enhance our capabilities to prevent, detect, and respond to threats as protecting our customers' data is at the core of our strategy.

Our information security organization is focused on achieving growth in maturity aligned to NIST CSF, modernizing our technology and capabilities as it aligns to the business and customer expectations, and a continued dedication in defending Thomson Reuters and protecting our customers data.

Security Organization

Program and Practices

Thomson Reuters has a global team of certified security and privacy subject matter experts dedicated to the security of Thomson Reuters products and services. This extended team is committed to our Information Security Risk Management (ISRM) Program, which is endorsed by the Thomson Reuters Executive Committee.

Our program and practices are aligned to NIST CSF and is achieved through the application of policies, standards, security controls at a level appropriate to the service provided and communicating appropriate security controls to application owners and technology teams across the business to support a secure product development and a secure operating environment. These processes help us to focus on the confidentiality, integrity, and availability of customer data that we store, process, or transmit.

We continue to enhance our offerings and participate in industry and government forums and groups, demonstrating our proactive approach to understanding and mitigating the threats we encounter while providing robust applications and services to our customers.

Policy and Standards

We have an internal policy governance process in place and our Information Security Risk Management team manages a set of information security policies and standards which outline information security and risk management principles that apply to our people, process, and technology practices. Additionally, we are focusing on continuous improvement. We regularly review and adapt our policies and standards to address changes to our products and services, evolving threats, regulatory changes, and our customers' information security expectations.

Our policies and standards are closely aligned with the ISO/IEC 27002:2017 and the NIST CSF to provide assurance globally of practices intended to ensure the confidentiality, integrity, and availability of our products and services. Further demonstrating our commitment to a secure operating environment is our ongoing certification program focusing on our strategic data centers and offices using the ISO/IEC 27001:2017 standard.

Organizational Structure

The Thomson Reuters global ISRM function is led by the Chief Information Security Officer (CISO), who is responsible for the protection of applications, platforms and infrastructure, as well as safeguarding our customers' data. We have built our organizational structure with information security at its core as seen in Diagram 1 below.

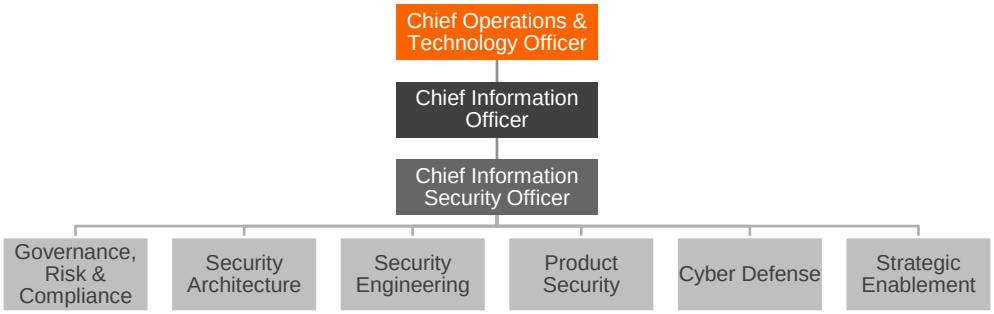

Diagram 1: Information Security Risk Management organizational structure

Our Employees

Thomson Reuters Code of Business Conduct and Ethics underscore our Trust Principles – integrity, independence, and freedom from bias.

Code of Conduct

All Thomson Reuters directors, officers, employees, and contingent workers are subject to a Code of Business Conduct and Ethics (the Code) and are required to acknowledge their consent to abide by its terms on an annual basis. The Code sets forth the highest ethical standards of conduct for how we operate in all the countries where we do business. The Trust Principles – integrity, independence, and freedom from bias – are incorporated into our Code and serve as a guide for anyone who encounters ethical questions while working for Thomson Reuters.

If misconduct is suspected, a report can be made to a supervisor, Human Resources, the ethics hotline, or our Chief Compliance Officer without fear of retaliation. Thomson Reuters will take prompt and appropriate action if it determines that a violation of the Code occurs, which may result in disciplinary action, up to and including termination of employment.

The Code also incorporates the Information Security Handbook, which describes the policies and guidance that must be followed when handling information or using Thomson Reuters assets or resources.

Background Screening

Employment background checks serve as an important part of Thomson Reuters' selection process. Verifying background information validates a candidate's overall employability or an employee's suitability for a particular assignment. Depending on the country and position at issue, all to the extent as is customary and permitted by law, Thomson Reuters' background checks may include identification verification, prior employment verification, criminal background information, global terror or sanctions checks and education verification.

Security Training

All employees, including contractors with access to Thomson Reuters systems and data, are required to complete an annual, mandatory Thomson Reuters Information Security and Privacy course. The security awareness team also conducts regular enterprise-wide phishing simulation exercises to all Thomson Reuters employees and contractors. Thomson Reuters designs phishing campaigns to increase secure behaviors within the organization.

Thomson Reuters delivers additional specialized training to specific groups of employees, as necessary. We also partner with third-party vendors to provide training resources to all skill levels through customized learning programs.

The Thomson Reuters Privacy Program is founded upon the Privacy Management Framework (PMF) and is overseen by a dedicated global Privacy Office.

Privacy Organization

Thomson Reuters places a high priority on meeting our customers' expectations of privacy. To meet these expectations, Thomson Reuters has a dedicated, global Privacy Office that is responsible for implementing, promoting, and overseeing a stringent Privacy Program that supports Thomson Reuters's compliance with applicable privacy and data protection laws around the globe. The Thomson Reuters Privacy Office is led by our Global Chief Compliance and Privacy Officer, who reports directly to the Chief Legal Counsel of Thomson Reuters, who in turn reports directly to our Chief Executive Officer.

Our Privacy Program is founded upon the Privacy Management Framework (PMF), formerly known as the Generally Accepted Privacy Principles (GAPP) framework, established by the Association of International Certified Professional Accountants (AICPA). The PMF is a principle-based framework comprised of the following nine principles with which Thomson Reuters strives to comply:

1. Management
2. Agreement, Notice and Communication
3. Collection and Creation
4. Use, Retention and Disposal
5. Access
6. Disclosure to Third Parties
7. Security for Privacy
8. Data Integrity and Quality
9. Monitoring and Enforcement

The Privacy Office operationalizes the principles of the PMF by establishing standards of conduct related to the protection and proper management of personal data, as well as monitoring and enforcing compliance with these policies and procedures. Our standards of conduct apply not only to our employees, but also to our dealings with third-party business partners. Members of the Privacy Office also collaborate closely within our customer segments and business lines to ensure that privacy issues and compliance risks are well understood and appropriately addressed in line with the requirements of the PMF.

Additional information about how we handle personal data, including how we address our responsibilities where we act as a data controller such as to manage requests from individuals who wish to exercise their rights of access, correction, amendment, and deletion, can be found in the Thomson Reuters Privacy Statement which is available online at: https://www.thomsonreuters.com/en/privacy-statement.html.

Compliance

Our ISRM compliance team performs assessments against policies, standards, and regulatory requirements and registers findings for review and remediation initiatives within the business. Thomson Reuters products each have a separate set of compliance attestations that are performed against it. Thomson Reuters completes the following assessments, although it will vary per product:

- SOC 1 and SOC 2 reports
- PCI-DSS
- ISO/IEC 27001:2017
- HIPAA
- SOX 404
- CJIS (roadmap)
- Cyber Essentials Plus (roadmap)
- Internal Controls Assessments against Thomson Reuters Policies

Thomson Reuters has built an enterprise risk management framework that incorporates cyber security risk assessments conducted on a semi-annual basis.

Cyber Risk Management

Thomson Reuters has dedicated resources focused on improving information security practices who strive to identify risks to our information assets and to guard against unauthorized access, loss, or misuse. As part of managing such risks, we use a variety of controls, security devices, monitoring tools, and threat models to analyze our systems and network.

Product and technology teams engage with information security subject matter experts to conduct architecture reviews, security penetration testing, vulnerability scans, application security testing, and technical compliance reviews to identify and mitigate security risks within Thomson Reuters.

Thomson Reuters has built an enterprise risk management framework that incorporates cyber security risk assessments conducted on a semi-annual basis. The enterprise risk framework includes governance procedures and management oversite for accepting risk associated to cyber security.

Cyber Risk Analytics and Security Ratings

Thomson Reuters is committed to meeting external cyber risk analytics and security ratings footprint as indicated by third-party scanning partners such as BitSight. We leverage a risk-based approach and a defined process to continuously monitor and address findings identified by BitSight as well as our internal processes and tools.

Data Security

Thomson Reuters maintains a Data Protection Services (DPS) program designed to minimize the cybersecurity, business and legal risk associated with intentional or unintentional data loss. The DPS Program accomplishes this by using data loss prevention technologies, engaging employees on proper data handling, and providing incident response on data handling violations.

Data Disclosures

Thomson Reuters takes its responsibilities as both a data controller and data processor very seriously and maintains a process to manage requests from individuals who wish to exercise their rights of access, as well as correction, amendment, and deletion.

More information can be found in the Thomson Reuters Privacy Statement which is available online at: https://www.thomsonreuters.com/en/privacy-statement.html.

Data Encryption

Thomson Reuters is committed to protecting our data and that of our customers and has employed data encryption in accordance with industry standards. Our encryption policies and standards are designed to preserve the confidentiality, integrity, and availability of data and to prevent unauthorized access, use or disclosure. Additionally, the policies and standards are designed to protect data while in transit or at rest.

Data Storing and Processing

Thomson Reuters uses several geographically dispersed data centers that are aligned to support our global businesses, including partnerships with multiple cloud service providers. Additionally, we leverage country-specific regions and hosting sites for some areas that are sensitive to latency and are aligned to contractual, legal, and regulatory requirements.

Thomson Reuters uses a data classification structure that sets forth the security controls for the management of customer data throughout its entire lifecycle.

Data Classification and Handling

At Thomson Reuters, protecting our customers' information is at the core of our Information security strategy. We use a data classification structure that sets forth the security controls for the management of customer data throughout its entire lifecycle. This includes creation, storage, use, sharing, archival and destruction of each data type.

We also have data handling guidelines designed to protect data. Some of our products and services are required to meet additional protection handling controls due to the sensitivity of information that is processed within them, or where specific regulatory requirements apply.

Data Retention

Thomson Reuters has a Record Management team which works in conjunction with the Privacy Office to implement appropriate rules and schedules relating to the retention of personal data. In determining data retention periods, Thomson Reuters takes into account local laws, contractual obligations, and the expectations of its customers.

Data Destruction

At the end of contract, customer data is returned in a manner and format mutually agreed to between the parties. Customer data will then be securely erased from Thomson Reuters servers.

Media Disposal

Thomson Reuters meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via barcodes and asset tags. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process. Physical destruction of disks is performed by a certified partner organization.

Identity and Access Management

Thomson Reuters employs identity and logical access security controls to the enterprise network and infrastructure, product environments, and applications for all employees, contractors, and third-party suppliers. Thomson Reuters have designed identity and Access controls to adhere to various established industry standards and best practices including principle of least privilege, segregation of duties, unique IDs, strong password creation and management, multi-factor authentication, and privileged access management. In addition, we conduct multiple internal and external assessments that evaluate access controls effectiveness within Thomson Reuters such as SOC 1, SOC 2, and ISO/IEC 27001:2017.

We use privileged access management to secure administrator access at the system level, which includes the use of multi-factor authentication. Privilege credential checkout is managed within the enterprise vault solution to ensure privileged accounts are vaulted, rotated and auditable to ensure accountability and traceability. Human Resource integration with downstream identity and access management platforms ensure immediate revocation of credentials for users exiting the organization.

Vendor Cyber Risk Management

The Thomson Reuters Vendor Cyber Risk Management Program which includes undertaking due diligence to ensure vendors and partners have the appropriate controls designed to protect our data and that of our customers. Third-party vendors are contractually required to comply with Thomson Reuters standards of conduct and controls applicable to data processors, which encompass both our security and privacy standards. Assurance assessments are conducted on vendors and third parties to verify compliance with these contractual terms.

Cloud Security

Thomson Reuters cloud deployments leverage security inherent to leading third-party cloud providers by utilizing native security services.

Thomson Reuters cloud deployments leverage security inherent to leading third-party cloud providers by utilizing native security services. Additionally, Thomson Reuters increases cloud defense in the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) environments by employing threat detection capabilities, as well as custom detection telemetry in key locations.

Applications deployed at Thomson Reuters are logically separated to better isolate risks associated with broad-based administrative access to cloud resources and data. Applications are deployed using repeatable processes, supporting a formal development lifecycle methodology designed to ensure cloud service provider account setup and ongoing maintenance is consistent and adheres to Thomson Reuters security policies and standards. Cloud applications are required to perform a standardized security assessment prior to production launch to validate its security requirements and ensure active controls are in place to protect cloud resources.

Our Cloud Compliance Security program leverages industry best practice tooling to scan the Thomson Reuters public cloud environments and provides controls to ensure the cloud configuration meets the Thomson Reuters policies and security architecture guidelines. This directly enhances Thomson Reuters' capabilities to ensure appropriate cloud configuration protocols are enforced and maintained within our public cloud estate.

Thomson Reuters leverages IaaS, SaaS, and Managed Services from the top public cloud providers in the industry today. As such, Thomson Reuters employs the shared responsibility model with these providers to protect Thomson Reuters' customer data. Thomson Reuters reviews the security capabilities of these cloud service providers on an annual basis to ensure they meet Thomson Reuters' security expectations.

Product Security

Thomson Reuters employs secure practices as part of the Software Development Life Cycle. Product development processes include key integration points with security infrastructure and architecture leads to guide security best practices throughout the build and development of applications and services. Internal and external vulnerability scans, as well as code scans and reviews are conducted on a regular basis.

Thomson Reuters employs a strategy of detective and preventative defensive security controls across our estate to achieve defense-in-depth against modern threats.

Network and Infrastructure Security

Thomson Reuters employs a strategy of detective and preventative defensive security controls across our estate to achieve defense-in-depth against modern threats. At critical locations within the network, technologies such as distributed denial of service mitigation, web application firewalls, next generation firewalls, intrusion detection systems and deep packet inspection are used to implement tiered network segmentation, route isolation, remote access control, and defensive visibility.

Robust secure configurations are created and deployed across our infrastructure and are based on industry best practices for configuration management. Technologies such as mobile device management, antivirus, endpoint detection and response, least privilege functionality, vulnerability scanning, phishing defense and encryption are used to provide a secure compute environment on which our users work, and products are hosted.

Physical Security

Our commitment to a secure operating environment is demonstrated by our ongoing certification program of our data centers' Information Security Management Systems (ISMS) to ISO/IEC 27001:2017.

Thomson Reuters data centers are managed to the standards within the Thomson Reuters Corporate Security Policy guidelines based on best practices in the industry.

Our guidelines include requirements for physical security, building maintenance, fire suppression, air conditioning, uninterruptible power supply (UPS) with generator backup, access to diverse power and communications, and closed-circuit television for internal and external monitoring. Thomson Reuters policy requires that our data centers be subject to an assessment periodically, which is measured by a grading system that determines the recovery level of the site. An evacuation test is also completed.

Thomson Reuters data center facilities are secured by computer-managed access control systems with security guards monitoring entrances. Visitors are required to sign in at building entrances and must have escorts within the buildings as well as appropriate badges. Multi-level security access is required for access to restricted areas e.g., ID cards, electronic access control incorporating proximity card readers, pin numbers, and/or biometric devices. Access is recorded, documented, and monitored across our data centers.

Other security controls are implemented across Thomson Reuters to physically secure the data centers and their assets. Access to delivery and loading areas is controlled and monitored, and deliveries and access are only allowed in those controlled areas.

Mobile Device Security

Thomson Reuters has a Mobile Device Management (MDM) Policy which sets forth security requirements and standards for use of devices such as smartphones and laptops. This includes an enforced policy, authenticated using device certificates for connection to the network, as well as the ability to set security controls per device and remotely wipe company data. Thomson Reuters does allow Bring Your Own Device (BYOD), but for an employee to use this they must agree to Thomson Reuters requirements as well as deploying the MDM solution to manage Thomson Reuters governed applications.

Security Defense and Response

Thomson Reuters currently follows a 24x7x365 Security Operations model with a global footprint.

Logging and Monitoring

Thomson Reuters performs automated and centralized logging of the different technology assets across our environment to provide real-time alerting, event correlation, and retroactive search capabilities. Elevated monitoring of key and strategic platforms within the organization adds an additional layer of defense designed to target key indicator sets and malicious behaviors to help better defend critical platforms and services. Thomson Reuters has deployed commercially available industry best practice SIEM (Security Information and Event Monitoring) solutions that are monitored by a 24x7 follow-the-sun Security Operations Center (SOC) team.

Security Operations

Thomson Reuters currently follows a 24x7x365 Security Operations model with a global footprint. Our SOC uses foundational and next-generation security tools and services designed to provide security monitoring and protection of our customers' data, assets, and operations around the globe.

Analytics, sensors, software agents, and vulnerability scanning tools are deployed across our data centers and cloud footprint to help detect, disrupt, or deny malicious activities, including spoofing, hijacking, malware, ransomware, and distributed denial of service. We utilize intrusion detection systems and other proactive security monitoring tools to help defend our operations 24x7. A dedicated team of security analysts provides continuous monitoring and analysis of the latest potential security threats to help identify and deflect malicious activities.

Security Incident Management

Thomson Reuters employs a tiered incident management and escalation model based on ITIL (Information Technology Infrastructure Library). Incidents are triaged based on criticality and assigned through incident leads. Incident command follows documented response practices, as well as established communications and escalation practices. Coordination of incidents is cross-functional and includes representation from many Thomson Reuters functions to ensure the proper handling of all incidents. Incident escalation procedures include pre-determined paths and notification protocols if required to the Thomson Reuters Board of Direction and Senior Management Team.

Key investigative staff are trained in forensics and investigative techniques and have developed the Thomson Reuters' Security Incident Response program that adheres to NIST CSF (NIST SP 800-61r2). The investigative response team employs a follow-the-sun model and engages in incident response and investigations 24x7. The team leverages third-party open-source tools, cots tools, and in-house developed proprietary tools and scripts to perform remote and on-site investigations. They employ industry best practices for forensic investigations such as chain of custody and evidence handling procedures for sensitive investigations such as privacy incidents.

Vulnerability Management

Thomson Reuters operates a vulnerability management process using a combination of commercially available industry leading tools to support a comprehensive application security and testing capability which include one or more of the following: static and dynamic application security testing, internal and external infrastructure vulnerability scanning and manual penetration testing.

Patch Management

Thomson Reuters' patch management standard follows industry best practices and product security principles which adhere to specific requirements wherein patches are communicated, rated, and deployed in an effective manner. The standard requires that technology teams deploy security patches based on their importance, and within specific time frames. We also employ forced patching protocols to mitigate unknown threats. Where required, additional Endpoint Protection security controls may be implemented to provide mitigation against known threats.

Endpoint Protection

Thomson Reuters takes the threat from malware to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware.

Our comprehensive endpoint protection strategy features antivirus scanners to protect against uploading and downloading malicious content. We deploy a combination of endpoint and antivirus solutions to prevent and detect both server and workstation environments to identify and prevent malicious code from reaching Thomson Reuters. The virus signature files are updated automatically, and our system administrators can also manually upgrade antivirus software as soon as important updates are available. Any update made to the virus software is validated and tested before being applied.

Cyber Intelligence

Thomson Reuters utilizes a range of commercial and open-source intelligence sources to enable our teams to continuously monitor, analyze, and mitigate potential cyber threats to the company. This intelligence includes indicators of compromise, attacker tactics and techniques, and changing motivations and targeting across threat groups. As new threat details are identified, we work to ensure our network and endpoint detection and prevention technologies are updated to better defend against these evolving threats.

The company also participates in strategic threat sharing forums and partnerships, which provide increased visibility into the latest threat trends observed across industries to which Thomson Reuters is aligned.

Business Resiliency

Our Business Continuity Plan prepares us to respond and recover from disruptive incidents such as natural disaster, pandemics, transit shutdowns.

Thomson Reuters has an established resilience strategy to ensure our continued ability to serve our customers, and to protect our people and assets. Our Business Continuity Plan (BCP) prepares us to respond and recover from disruptive incidents including but not limited to natural disaster, pandemics, transit shutdowns. The BCP itself is company confidential and not provided to customers, however, we are able to provide a high-level statement to customers about our BCP upon request. In many disaster scenarios, workforce disruptions are expected and our comprehensive plan accounts for this. Additionally, the business continuity risks that could impact operations continue to evolve, and we endeavor to stay current with industry best practices and the recommendations of the business communities in which we work.

We prioritize systems recovery based on the criticality of the systems to our customers; then recovery requirements are established based on those priorities. As a further safeguard, many critical functions can be transferred to out-of-region locations. Additionally, Thomson Reuters has the ability to support many critical functions by enabling designated staff to work from their homes through secure remote-access connections.

Asset Management

Thomson Reuters strives to protect its information technology assets and data by implementing and maintaining appropriate asset management business practices and technology across the enterprise including asset identification and classification, infrastructure and software asset inventory management, acceptable use, asset decommission and disposal.

Thomson Reuters maintains a centralized inventory of both hardware and software which is supplemented by documentation detailing the purpose and business criticality of each asset. Assets held within the inventory have an assigned owner with the responsibility of maintaining the asset attributes.

Change Management

Thomson Reuters maintains a change control process based on ITIL best practices. The process is designed to ensure a formal development lifecycle methodology is used to manage changes and provide assurance throughout the technology lifecycle.

The process enables beneficial changes to be made with minimum disruption to business operations, ensuring the best possible levels of service quality and availability are maintained. This is accomplished through a formal approach to plan, coordinate, schedule, approve, assess the risk and potential impact, and track all changes introduced to a controlled environment in a manner that protects their ability to deliver services. Software, configuration, and hardware changes may involve, but are not limited to, databases, network connectivity, implementation of new hardware, and updates to existing hardware.

For More Information

Contact your Thomson Reuters Representative for more information.

- About Corporate Governance visit our Investor Relations site at: https://ir.thomsonreuters.com/
- View or download our Code of Business Conduct and Ethics at: https://ir.thomsonreuters.com/corporate-governance/code-conduct
- About our products, visit https://thomsonreuters.com/
- Our Procurement Guide describing customer contracting policies and is available at: https://www.thomsonreuters.com/en/resources/thomson-reuters-procurement-guide.html
- Contact your Thomson Reuters Representative or contact us online at: https://thomsonreuters.com/contact-us