THOMSON REUTERS®

Thomson Reuters
Information Security Principles

September 2021

White Paper

Last Updated September 2021

Table of Contents

Last Updated September 2021

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

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.

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.

Protecting our customers' information is at the core of our Information Security strategy. We have established policies and a governance structure designed to mitigate and respond to potential security risks.

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

Organization

Program and Practices

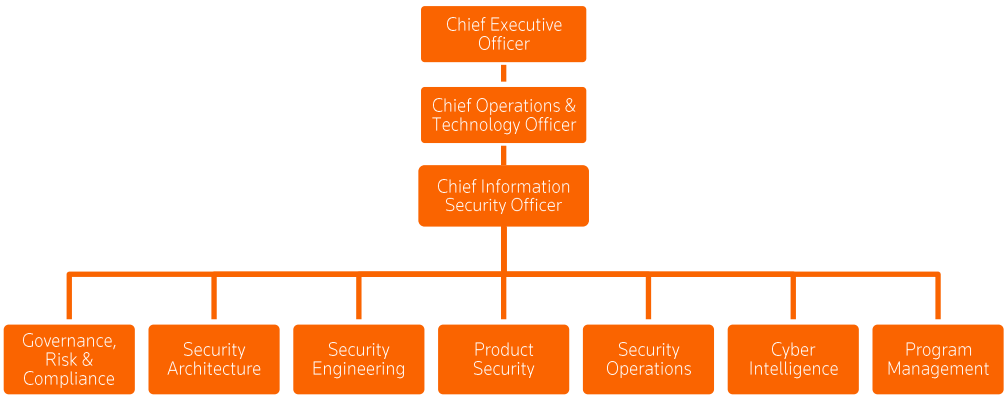
Thomson Reuters has a global team of certified security and privacy subject matter experts dedicated to the security of Thomson Reuters products and services. This extended team is committed to our Information Security Risk Management program, which is endorsed by the Thomson Reuters Executive Committee.

Our strategy leverages a risk-based approach aligned with the International Organization for Standardization (ISO), and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) In this way we ensure alignment with business priorities and customer need while adhering to best practices. We achieve this through the application of policies, standards, and supporting security controls at a level appropriate to the service being provided, along with communicating appropriate security controls to application owners and technology teams across the business to support the secure development of products 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 are involved 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.

Organization Structure

Our global Information Security Risk Management (ISRM) function, led by the Chief Information Security Officer (CISO), is responsible for ensuring the protection of applications, platforms, and infrastructure, and safeguarding our customer data. We have built our organizational structure with information security at its core, which you can see below:



Last Updated September 2021

THOMSON REUTERS®

Policy and Standards

We manage 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, in an ongoing practice 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 International Organization for Standardization (ISO/IEC 27002:2013) and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). We align our information security policies and standards to these standards 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 27001:2013 standard.

Thomson Reuters Code of Business Conduct and Ethics underscore our values of Trust, Partnership, Innovation and Performance.

Our Employees

Code of Conduct

All Thomson Reuters employees, officers and directors and our majority-owned or controlled subsidiaries, as well as consultants, temporary employees, and agents performing services for us on our behalf (such as our business partners) are subject to a Code of Business Conduct and Ethics, which sets forth the standards of conduct that apply to our employees in all the countries where we do business. The Code underscore our values of Trust, Partnership, Innovation and Performance, and all employees are required to acknowledge their consent to abide by its terms on an annual basis.

We enforce employee adherence to our Code, and failure to adhere to it will lead to disciplining employees, where appropriate, up to and including termination of employment. Thomson Reuters will at times use contract employment agencies, which are required to ensure their employees sign the Code, a nondisclosure agreement which specifies and extends client confidential requirements and an approved contract.

The Code 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. These policies apply to all officers, directors, and employees of Thomson Reuters Corporation and its subsidiaries, as well as outside consultants, contractors, temporary employees, and agents engaged by Thomson Reuters when performing services for, or on behalf of, Thomson Reuters.

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.

Training

All employees (and contractors with access to the Thomson Reuters systems and data) must complete an annual, mandatory Information Security course. Employees are also required to complete the Thomson Reuters online Privacy course.

Additional specialized training is delivered to particular groups of employees as necessary. We also partner with third party vendors to provide training resources to all skill levels through customized internal programs.

The security awareness team also conducts regular enterprise-wide phishing simulation exercises to all Thomson Reuters employees and contractors. Phishing campaigns track metrics on progress toward increasing secure behaviors within the organization.

Asset Management

Thomson Reuters strives to protect its IT 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, asset monitoring, 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.

Risk Assessment and Treatment Plan

With dedicated resources focused on improving information security practices throughout Thomson Reuters, we 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 regularly to obtain risk assessment services. The services performed during risk assessment activities may include architecture reviews, security penetration testing, vulnerability scans, application security testing, and technical compliance reviews.

Following risk assessment activities, Thomson Reuters Information Security Risk Management team, to the extent required, consults with product and technology teams to develop remediation plans and roadmaps to address gaps in compliance, or areas of identified risk.

Additionally, our internally focused compliance team partners with third party auditors to evaluate the effectiveness of our security controls and register findings for review and remediation initiatives.

Last Updated September 2021

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 Privacy Management Framework 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 Privacy Management Framework.

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.

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

Data Security

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 management of customer data throughout its entire lifecycle. This includes creation, storage, use, sharing, archival and destruction of each data type.

There are also data handling guidelines designed to ensure data is protected. Some 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.

Last Updated September 2021

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.

Data Protection

Thomson Reuters maintains a data protection program focused on protecting company and customer data from loss or exposure. Thomson Reuters data protection program accomplishes this through the use of 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. For more information, see the Thomson Reuters Privacy Statement at https://www.thomsonreuters.com/en/privacy-statement.html.

Retention

Thomson Reuters has a Records 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.

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. Identity and Access controls are designed to adhere to various established industry standards and best practices including principle of least privilege, segregation of duties (SoD), unique IDs, strong password creation and management, multi-factor authentication (MFA), and privileged access management.

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 (HR) integration with downstream Identity and Access Management (IAM) platforms ensure immediate revocation of all credentials for users exiting the organization.

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. Software, configuration, and hardware changes may involve, but are not limited to, databases, network connectivity, implementation of new hardware, and updates to existing hardware.

Network and Host 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 (DDoS) mitigation, web application firewalls, next generation firewalls, intrusion detection systems (IDS) and deep packet inspection are used to implement tiered network segmentation, route isolation, remote access control, defensive visibility, and supply chain risk mitigation.

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, anti-virus, endpoint detection and response, least functionality, vulnerability scanning, phishing defense and encryption are used to provide a secure compute environment on which our users work, and products are hosted.

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

Security Operations

Thomson Reuters currently follows a 24x7x365 Security Operations model with a global footprint. Our Security Operations Center (SOC) uses foundational and next-generation security tools and services designed to provide security monitoring and protection of our people, 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 (DDoS). We utilize intrusion detection systems (IDS) and other proactive security monitoring tools to help defend our operations 24/7. A dedicated team of security analysts provides continuous monitoring and analysis of the latest potential security threats to help identify and deflect malicious activities.

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. Targeted or elevated monitoring of key and strategic platforms within the organization adds an additional layer of defense designed to target key indicator sets, behaviors, or abuse scenarios, to help better defend critical platforms and services.

Thomson Reuters cloud deployments leverage security inherent in cloud platforms and by utilizing the native security services.

Cloud Security

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 IaaS, PaaS, and SaaS environments by employing threat detection capabilities, as well as custom detection telemetry in key locations. Thomson Reuters applications are separated by business segment 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 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.

Last Updated September 2021

Product Security

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. In addition, Thomson Reuters Information Security Risk Management team supports a comprehensive application security testing capability which can include one or more of the following: services to perform static and dynamic application security testing, internal and external infrastructure vulnerability scanning, and third-party penetration testing.

Our 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. Where required, additional security controls may be implemented to provide mitigation against known threats.

Where appropriate or required by law, Thomson Reuters product teams will engage with independent third parties to perform assessments on select products, primarily in the category of SSAE18/SOC audits and ISO/IEC 27001:2013.

Cyber Intelligence and Threat Detection

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. Threat hunting activities are also conducted to help identify threats within the Thomson Reuters environment.

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.

The goal of our Business Continuity and Disaster Recovery strategy and plans is to ensure our continued ability to serve our clients, and to protect our people and assets.

Business Resiliency

Framework

Like other large multinational corporations, Thomson Reuters is exposed to an increasing array of potential risks that could impact critical business functions or services following a disruptive incident. The goal of our Business Continuity and Disaster Recovery strategy and plans is to ensure our continued ability to serve our clients, and to protect our people and assets. We have an established global, structured framework designed to be prepared should a disruptive incident occur. This approach addresses disruptions of varying scope, including, but not limited to, large-scale location-specific events and Thomson Reuters-only disruptive incidents.

Business Planning

Central to our efforts is a requirement that each Thomson Reuters business unit develop, test, and maintain business continuity plans for each of its critical functions. We strategically leverage our global resources and infrastructure by relocating impacted business units to designated and tested business continuity sites, and by redeploying critical resources, data, and systems between geographically dispersed data centers and sites, based on business requirements, and as dictated by the specific crisis event. In accordance with business requirements, and as part of our regular maintenance, we schedule periodic testing of systems failover/recovery and business continuity sites and plans, increasing the confidence of our business continuity readiness. Associated strategies and plans are required to be reviewed and updated, at a minimum, on an annual basis.

Last Updated September 2021

Prioritization

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 is able to support many critical functions by enabling designated staff to work from their homes through secure remote-access connections.

Incident Response

Thomson Reuters employs a tiered incident management and escalation model based on ITIL. Incidents are triaged based on criticality and assigned through incident leads. Incidentcommand follows documented response practices, as well as established communications and escalation practices. Coordination of incidents also involve IT and product teams and the use of outside communications expertise and legal counsel where appropriate.

Vendor Risk Management

The Thomson Reuters Vendor Risk Management Program 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 testing and audits are carried out on vendors and third parties to verify compliance with these contractual terms.

Thomson Reuters data centers are managed to standards based on best practices in the industry.

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 27001:2013. We are also members of the Uptime Institute with Tier 2 and 3 designed facilities and have received multiple continuous availability awards at our sites.

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.

Last Updated September 2021

Compliance

Our ISRM compliance team performs audits against policies, standards, and regulatory requirements and registers findings for review and remediation initiatives within the business. Based on the ISO 27001:2013 requirements, we use a risk-based approach assessing key products, applications, and data centers focusing specifically on information protection, including:

- Annual self-assessments
- ISO audits and risk assessments
- SOC1 and SOC2 reports (based on business need)
- Internal assessments

Mobile Device Management

Thomson Reuters has a Mobile Device Management 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.

For More Information

More about Corporate Governance on our Investor Relations site at: https://ir.thomsonreuters.com/
Read about our products at: https://thomsonreuters.com/

You may download a copy of our Code of Business Conduct and Ethics at https://ir.thomsonreuters.com/corporate-governance/code-conduct

Our Procurement Guide describing customer contracting policies is available at https://www.thomsonreuters.com/en/resources/thomson-reuters-procurement-guide.html

Contact us: https://thomsonreuters.com/contact-us

Last Updated September 2021

THOMSON REUTERS®