THOMSON REUTERS®

Thomson Reuters
Information Security Principles

January 2021

White Paper

Table of Contents

Organization 3
- Program and Practices 3
- Organization Structure 3
- Policy and Standards 3

Our Employees 4
- Code of Conduct 4
- Background Screening 4
- Training 4

Asset Management 4

Risk Assessment 5

Privacy Organization 5

Data Security 6
- Classification and Handling 6
- Storing and Processing 6
- Data Disclosures 6
- Retention 6

Identity and Access Management 6

Change Management 6

Network and Host Security 7

Security Operations 7

Logging and Monitoring 7

Cloud Security 7

Product Security 8

Cyber Intelligence and Threat Detection 8

Business Resiliency 8
- Framework 8
- Business Planning 8
- Prioritization 9

Incident Response 9

Vendor Risk Management 9

Physical Security 9

Compliance 10

Mobile Device Management 10

For More Information 10

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

Thomson Reuters maintains its 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. It is designed to answer questions about how Thomson Reuters protects customer data.

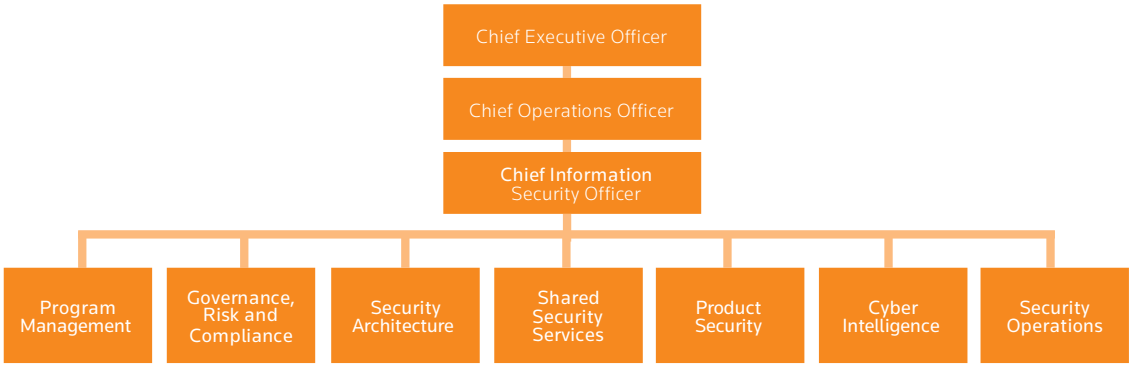
Organization

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 is to use a risk-based approach aligned with the International Organization for Standardization (ISO) Framework to address our compliance requirements. 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 sensitive customer data which 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. As a result, we have built our organizational structure with information security at its core, which you can see below:



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 international standard ISO/IEC 27002:2013. We align our information security policies and standards to this international standard to provide assurance globally of practices that 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 using the ISO 27001 standard.

Thomson Reuters Code of Business Conduct and Ethics is founded on our Trust Principles of integrity, independence, and freedom from bias.

Our Employees

Code of Conduct

All Thomson Reuters employees are subject to a Code of Business Conduct and Ethics, which sets forth the laws, rules, and standards of conduct that apply to our employees in all the countries where we do business. The Code is founded on our Trust Principles of integrity, independence, and freedom from bias, and all employees are required to acknowledge their consent to abide by its terms.

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

Subject to applicable local law, Thomson Reuters employees and contractors must complete pre-employment background screening checks and comply with confidentiality agreements. Thomson Reuters retains copies of this background screening documentation. Each employee receives access to the appropriate premises and systems upon completion of these checks, and controls are in place to monitor and review access. Should the employee leave, access to systems and premises are ceased as per the Thomson Reuters Leaver Policy.

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 by the Thomson Reuters Privacy Office 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 such as the "Thomson Reuters Cloud Learning Pathway" and "Thomson Reuters Application Assurance Academy" which concentrate on cloud implementations and secure software development, including design, coding, testing, and implementation.

Asset Management

Thomson Reuters protects its IT assets and data by implementing and maintaining appropriate asset management business practices 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

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, and monitoring tools to analyze our systems and network. Our policies and standards are closely aligned with international standard ISO/IEC 27002:2013. Product and technology teams engage with information security subject matter experts regularly to obtain risk assessments services. The services performed during risk assessment activities include architecture reviews, 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 performs audits against policies, standards, and regulatory requirements, and registers findings for review and remediation initiatives within the business.

Thomson Reuters has a dedicated, global Privacy Office that is responsible for implementing, promoting, and overseeing a stringent Privacy Program framework.

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 framework that supports Thomson Reuters's compliance with applicable privacy and data protection laws around the globe. This Thomson Reuters Privacy Program is comprised of numerous controls and procedures to appropriately safeguard personal data across the enterprise, including:

- Operationalizing, into our privacy practices, the Thomson Reuters Code of Business Conduct and Ethics, which sets out the standards of conduct that apply to all employees in all countries where we do business and which is founded upon our Trust Principles of integrity, independence, and freedom from bias.
- Formally documenting and implementing privacy policies and procedures related to the protection and proper management of personal data. Additionally, our Privacy Statement can be found here.
- Establishing and enforcing appropriate measures – including proper vetting procedures and contractual requirements – when engaging and providing access to personal data to sub-processors, contractors, and third parties acting on our behalf, as well as when transferring personal data across borders.
- Training of employees and contractors to provide the organization with an awareness of the Thomson Reuters Privacy Program, as well as an understanding of each employee's individual responsibility to safeguard and properly handle personal data.
- Tracking and addressing new and upcoming changes to data protection laws that affect Thomson Reuters in a manner that is agile and scalable.

The Thomson Reuters Privacy Office is led by our Global Chief Privacy Officer (CPO). Our CPO reports directly to the Chief Legal Counsel of Thomson Reuters, who in turn reports directly to our Chief Executive Officer.

Members of the Privacy Office 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 operational and regulatory requirements.

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

Data Security

Classification and Handling

Thomson Reuters uses a three-tiered (Strictly Confidential, Confidential, or Public) classification structure that sets forth the security controls for management of customer data throughout its entire lifecycle. This includes ownership, storage, destruction, and transfer of each data type.

There are also data handling guidelines to ensure data is protected. Some products and solutions are required to meet additional protection handling controls due to the sensitivity of personally identifiable information that is processed within them or because they are subject to specific regulatory requirements, such as General Data Protection Regulation (GDPR), or the Payment Card Industry Data Security Standard (PCI DSS).

Storing and Processing

Thomson Reuters uses several geographically dispersed data centers that are aligned to support our global businesses. This also includes partnership with cloud service providers, such as Amazon Web Services and Microsoft Azure, for cloud solutions. Additionally, we leverage country-specific sites for areas that are sensitive to latency or have detailed regulatory requirements.

Data Disclosures

Thomson Reuters takes its responsibilities as a data controller 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 athttps://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 enforces identity and access security controls to enterprise resources, product environments, and applications. These controls adhere to established industry standards and best practices including least privilege, segregation of duties, unique IDs, password management, strong authentication, and privileged access management.

Thomson Reuters employs Privileged Access Management to secure administrator access at the system level. This adds multi-factor authentication and limited credential life span to reduce the risk of administrative account compromise. Capabilities integrated with privileged access management remove access automatically when employee leaves the company.

Change Management

Thomson Reuters maintains a Change Control Policy to ensure a formal Systems Development Life Cycle (SDLC) methodology is used to manage changes and provide assurance throughout the technology life cycle. 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 blended strategy of passive, interactive, and proactive defensive technologies across our environment to help improve defense in-depth wherever possible. This includes, but is not limited to, network segmentation and route isolation in key or strategic locations of the network, sensor, and defensive technologies at critical choke points or network interconnects (e.g., firewalls, anti-virus, host management, vulnerability scanning, and phishing defense), and a response doctrine that addresses network and host-specific risks.

Standard security builds are deployed across our infrastructure and based on industry practices for secure configuration management. Our proactive defenses vary by product type, and can include appropriate server maintenance, system hardening, and encryption (in transit and at rest).

Security Operations

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

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 to provide security monitoring and protection of our people, assets, and operations around the globe.

Analytics, sensors, software agents, and vulnerability scanners tools are deployed across our data centers and cloud footprint to help detect, disrupt, or deny malicious activities, including spoofing, hijacking, and denial of service (DoS). We also employ intrusion detection systems (IDS) and have other proactive security monitoring tools in place to help defend our operations 24/7. A dedicated team of security analysts provides continuous monitoring and analysis of the latest security threats to help identify and defect malicious activities

Logging and Monitoring

Thomson Reuters monitors systems, services, and operations to ensure the health of the operating environment on which our applications run. Automated and systemic security logging of the operating environment is ongoing for the purpose of real-time awareness, event correlation, and incident response. 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.

Cloud Security

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

Thomson Reuters cloud deployments leverage security inherent in cloud platforms and by utilizing the native security services. Additionally, Thomson Reuters increases cloud defense in the IaaS, PaaS, and SaaS environments by employing Amazon GuardDuty and Azure Security Center, as well as custom detection telemetry in key locations. Thomson Reuters applications are separated and by business segment to better isolate risks associated with broad-based administrative access to cloud resources and data. All accounts builds are automated to ensure every account is setup uniformly to adhere to Thomson Reuters security requirements. Automated checks are regularly done to ensure critical security requirements are maintained.

All cloud applications are required to perform a security assessment prior to production launch to validate all security requirements and ensure active controls are in place to protect cloud resources.

Product Security

Product development teams regularly consult with information security subject matter experts to assist with building security into their 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.

The patch management standard follows industry best practices by requiring that 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 SSAE/SOC audits.

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 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 ensure that Thomson Reuters is 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 conduct stringent testing of systems failover/recovery and business continuity sites and plans on a recurring basis, 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.

Prioritization

We prioritize systems recovery based on the criticality of the systems to our clients; 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 in each region. Incident command 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 general counsel where necessary.

Vendor Risk Management

The Thomson Reuters Vendor Risk Management Program includes undertaking due diligence to ensure vendors and partners have the appropriate controls in place to protect our data and that of our customers. Third parties are contractually required to comply with the Thomson Reuters Data Processor Obligations (DPO), which encompass both our security and privacy standards. Assurance testing and audits are carried out on vendors and third parties to verify ongoing compliance with contractual terms and the DPO.

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 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 traffic 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.

Compliance

Based on the ISO 27001 requirements, we use a risk-based approach assessing key products, applications, and data centers focusing specifically on information protection, including:

- Annual self-assessment
- ISO audits and risk assessments
- Internal assessment

Our ISRM compliance team performs audits against policies, standards, and regulatory requirements, and registers findings for review and remediation initiatives within the business. Additionally, we maintain an ongoing external attestation program across our strategic products and data centers.

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

Thomson Reuters

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 https://thomsonreuters.com and for the latest world news, https://reuters.com.

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

Last updated January 2021.

TR827619_09/2019_DGM

THOMSON REUTERS®