Thomson Reuters ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting

Information Security White Paper

February 2018

the answer company™
THOMSON REUTERS®

ONESOURCE® Trust Tax provides wealth managers with an integrated compliance solution that automates the fiduciary tax process from data management to 1099 and 1042-S reporting. To accomplish this, our software interfaces with trust accounting systems. ONESOURCE Trust Tax automates the fiduciary tax process and handling of returns, including estimates. We also offer Web delivery of tax documents, which can save time and money by giving beneficiaries direct access to their information and documents.

ONESOURCE Tax Information Reporting software and services offer corporations a complete U.S. federal and state solution, as well as a Canadian solution, which includes TIN Compliance, withholding management and industry training.

Thomson Reuters maintains its reputation for providing reliable and trustworthy information through a variety of means, including an information security management framework supported by a wide range of security policies, standards and practices.

This document explains our approach to information security for ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting. It is designed to answer questions our customers regularly ask.

Thomson Reuters is the world's leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. Thomson Reuters shares are listed on the Toronto and New York Stock Exchanges (symbol: TRI).

At Thomson Reuters, protecting our customers' information is at the core of our Information Security strategy. We have established policies and a governance structure to mitigate and respond to potential security risks.

We align ourselves to multiple security and risk frameworks and assess the effectiveness of our security program on an ongoing basis. We are committed to providing a secure environment for the personal data and confidential information we hold.

Security Policy

Our Information Security policy, aligned to the NIST Cybersecurity Framework, is endorsed by the Thomson Reuters Executive Committee. This policy mandates the security principles that apply to our people, process and technology. These policies and supporting standards are reviewed and updated as necessary to take into account evolving technical risks as well as regulatory changes and our customers' needs for information security.

Organizational Security

Our global Information Security Risk Management (ISRM) function is responsible for ensuring applications, platforms and infrastructure are protected and our customer data is safeguarded. The ISRM team is led by the Chief Information Security Officer (CISO).

Thomson Reuters places security at the heart of what we do. As a result, we have built our organizational structure with information security at its core, which you can see below.

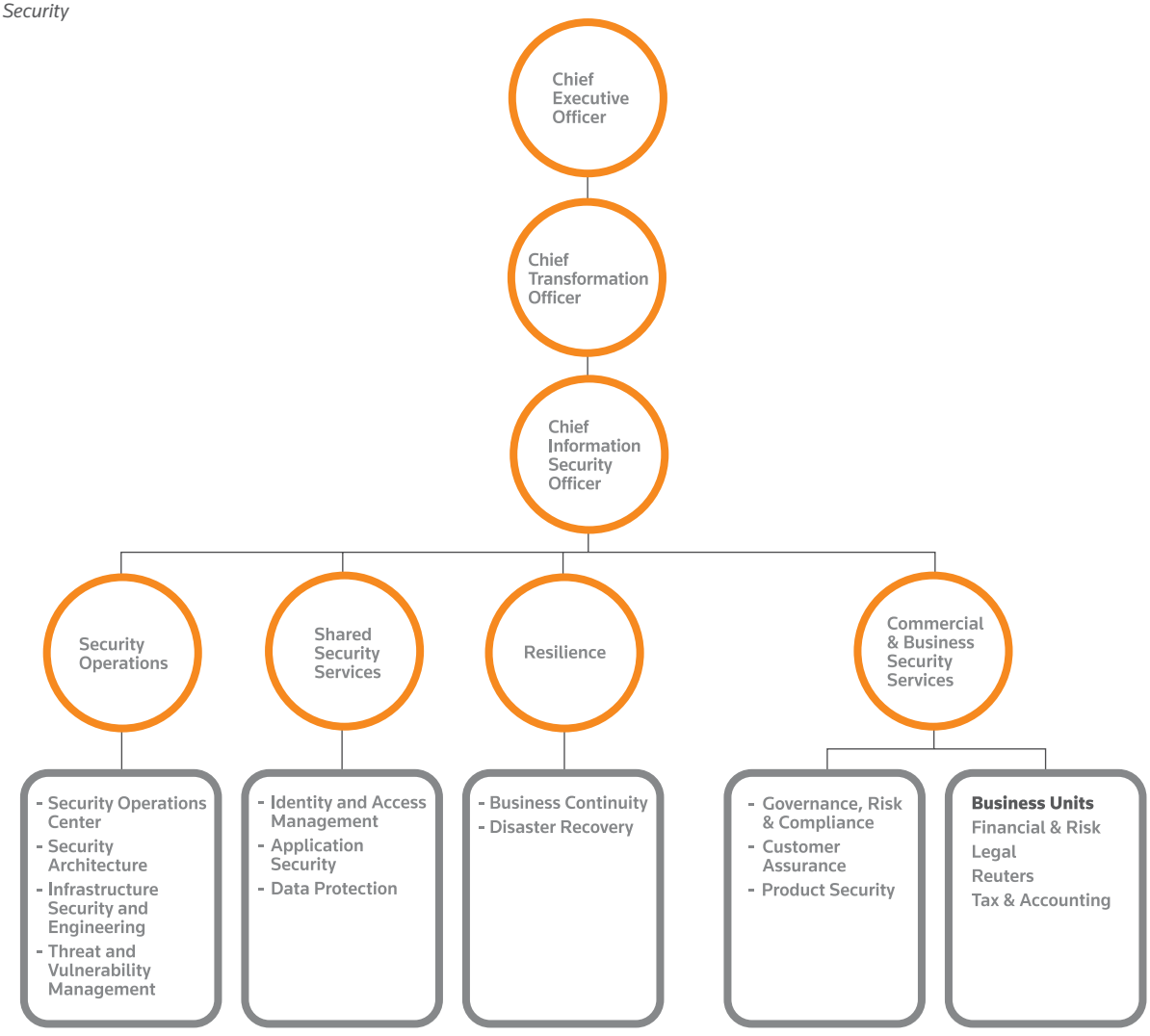
Risk Assessment and Treatment

We use a risk-based approach across our security programs. The ISRM team maintains a risk framework that sets forth the requirements and responsibilities for risk identification, registration and treatment. Identified risks are submitted into a central repository.

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 product and technology teams engage information security-subject matter experts regularly to provide risk assessment services. Architecture reviews, vulnerability scans, application security testing and technical compliance reviews are several of the services performed during risk assessment activities for ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting. Following risk assessment activities, our ISRM team consults with product and technology teams to develop remediation plans and road maps to address gaps in compliance or areas of identified risk.

Organizational Security



Asset Management

Our asset management program is based on Information Technology Infrastructure Library (ITIL) disciplines and is subject to our ISO 27001 certification. A centralized inventory of hardware and software is maintained and supplemented by detailed documentation regarding the purpose of each type of asset and its criticality to the business. Assets held within the inventory have an assigned owner with the responsibility of maintaining the asset attributes.

Employees and Contractors

Employees are required to complete training on the company's Code of Business Conduct and Ethics. The Code sets forth the laws, rules and standards of conduct that apply to our employees in countries where we do business. We enforce this Code as appropriate, up to and including dismissal.

In addition, when we hire through contract employment agencies, contractors are required to read and sign the Thomson Reuters Code of Business Conduct and Ethics, sign a nondisclosure agreement (which specifies and extends client confidential requirements), and agree to the applicable standard contractual terms and conditions.

Thomson Reuters employees must complete pre-employment background screening checks and comply with confidentiality agreements. Each employee is provided access to the appropriate premises and systems upon completion of these checks. Controls are in place to monitor and review access. Should the employee leave, access to systems and premises are ceased as per Thomson Reuters Leaver Policy.

Physical and Environmental Security

Our commitment to a secure operating environment is demonstrated by our ongoing certification program of our strategic data centers' information security management systems (ISMS) to ISO/IEC 27001 and ISO 9001.

Thomson Reuters data center facilities are secured by computer-managed access control systems; security guards also monitor entrances. Visitors are required to be signed in and escorted as well as have appropriate badges. Multilevel security access is required for access to restricted areas. 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 controlled areas.

Thomson Reuters data centers are managed to the standards within 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, and access to diverse power and communications. 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 and an evacuation test is completed.

Operations Management

Thomson Reuters employs a formal process to notify clients in writing prior to certain and defined changes which may impact their service.

The ONESOURE Trust Tax solution has an automated backup system configured to perform incremental and full backups for production data. Backups are kept on-site in Thomson Reuters data centers and replicated between sites. There is no off-site backup media. Backup processes run daily and data is stored onsite for 45 days.

Thomson Reuters uses a third-party service provider for destruction of end-of-life electronic media devices. The supplier follows BS 8470 and is certified to ISO 9001.

User Data Storage and Segregation

ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting data is stored in a multi-tenant environment, logically segregated via a database schema and role-based access control to ensure protection from unauthorized access. Data is encrypted at rest via AES 256-bit.

Identity and Access Management

Thomson Reuters enforces identity and access controls to enterprise resources, product environments and applications with adherence to established industry standards including least privilege, segregation of duties, unique IDs, password management and privileged access management.

Thomson Reuters employs Privileged Account 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 account management remove access automatically when employee status changes.

Access to production networks and production systems is governed by technical controls that require multi-factor authentication and unique IDs.

ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting employ Thomson Reuter's Identity and Access controls and regularly review administrative access to enterprise resources, product environments and applications.

ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting users must be authenticated to the ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting Web-based application interface with a unique ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting user ID and password. A single sign-on configuration is also available via SAML or MS ADFS.

Change Management

A formal Systems Development Life Cycle (SDLC) is adopted and applied for our development efforts, including ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting.

We have a formal Change Control Policy and Procedure in place. Items considered for Change Control are tracked through a formal process. Operational and code changes are included in the change

control process. This can involve database changes, network connectivity changes, implementation of new hardware and changes to existing hardware.

We have an established process around changes, which is considered and tested prior to implementation.

Security Operations

Thomson Reuters currently follows a 24x7x365 "follow the sun" Security Operations model with a global response footprint and a main Cyber Fusion Center located in Richmond, VA. Our Security Operations Center (SOC) utilizes foundational, advanced 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, vulnerability scanners and application white-listing tools are deployed across data centers 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 defeat malicious activities, and cyber hunters are employed to help address asymmetric threats.

Monitoring Coverage

In addition to environmental defense, Thomson Reuters employs targeted or elevated monitoring to key or strategic platforms within the organization. This additional layer of defense is designed to target key indicator sets, behaviors or abuse scenarios, to help better defend critical platforms and services.

Incident Event and Communications Management

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. Incident coordination also works with existing IT and product escalation practices where necessary, including the use of outside communications expertise and general counsel where deemed necessary.

Network & 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 response doctrine that addresses network and host-specific risks. Proactive defense can include appropriate server maintenance, the use of encryption and hardening.

Cloud Security

Thomson Reuters employs both standard, native cloud defense functions in IaaS, PaaS and SaaS environments, as well as custom detection capabilities in key locations.

Thomson Reuters is also employing segmented account management in IaaS containers to better isolate risks associated with broad-based administrative access to cloud consoles and account services.

Additionally, we are working to deploy analytic-based defense capabilities to help better identify and respond to threats in multi-cloud formations.

Threat Management / Cyber Intelligence

Thomson Reuters employs a wide range of commercial and Open Source Intelligence indicator feeds and flows to help ensure our detection technologies are kept current with the latest cyber intelligence indicators. This is important because threats are asymmetric and require constant vigilance and updates to ensure intelligence indicators are refreshed. The company also participates in strategic-threat-sharing forums and partnerships to ensure our teams are kept up to date on the latest exploits and techniques in cybersecurity.

In addition to threat intelligence, we employ a range of host- and network-based vulnerability scanning capabilities to assess risks to our estate. Remediation of vulnerabilities is handled through a review practice, and criticality scores are assigned to vulnerabilities to help ensure timely response in corrective actions.

Thomson Reuters leverages hunting functions to help augment standard incident response doctrine and to proactively help identify the latest and most significant threats.

As new risks are identified, Thomson Reuters is constantly striving to mitigate these evolving threats.

Business Resiliency

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.

Central to our efforts is a requirement that each Thomson Reuters business unit develops, tests and maintains business continuity plans for each of its critical functions. Our strategy and plans include leveraging our global resources and infrastructure through relocating impacted business units to designated and tested business continuity sites, and 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.

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 can support many critical functions by enabling designated staff to work from their homes through secure remote-access connections. Integral to our business continuity readiness is employee awareness and training so that employees are aware of their roles and responsibilities in the event of a disruptive incident. In accordance with business requirements, and as part of our regular maintenance, stringent testing of systems failover/recovery and business continuity sites and plans is conducted on a recurring basis, which increases 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.

Oversight of our preparedness and readiness is provided by our Executive Committee. We have dedicated business continuity teams in EMEA, Americas and Asia. This group monitors the development, implementation, maintenance and testing of each of our business unit strategies and plans, and drives globally continuous improvement.

In the event of an incident or significant disruption, our Thomson Reuters Service Centers, Service Alerts and customer communication channels will be used to provide proactive information to our customer base, in addition to direct contact via Account Management teams.

Compliance

Based on the ISO 27001 requirements, we have implemented a program of internal risk assessments 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.

ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting are also subject to an annual SOC1 Type 2 and SOC 2 type 2 audit.

Encryption

ONESOURCE Trust Tax and ONESOURCE Tax Information Reporting data and metadata are encrypted using TLS during transit. At rest, data and metadata are encrypted using AES encryption. Optional SFTP transfers are encrypted via PGP. ONESOURCE Trust and Tax Information Reporting also have exposed a client-accessible SOAP Web service API using the .NET WCF framework. The services are standards-compliant in order to promote interoperability with other platforms and are secured by WS-Security (X.509 Certificate Token Profile) in conjunction with HTTPS.

Mobile Device Management

Mobile devices such as smartphones and tablets are managed through a formal Mobile Device Management program with an enforced policy authenticated using device certificates for connection to the network. This includes the ability to set security controls and remotely wipe company data from a mobile device.

For more information:

More about Corporate Governance on our Investor Relations site at: **http://ir.thomsonreuters.com/**

Read about our products at: **http://thomsonreuters.com/**

For ONSOURCE Trust Tax and Tax Information Reporting Customer Support, please visit: **https://tax.thomsonreuters.com/support/onesource/customer-center**

Contact us: **http://thomsonreuters.com/contact-us/**

The intelligence, technology and human expertise you need to find trusted answers.

the answer company™ THOMSON REUTERS®