THOMSON REUTERS®

Confirmation NextGen, part of Thomson Reuters

Information Security Summary

Product Documentation

This document explains Thomson Reuters' approach to information security and data privacy for **Confirmation NextGen**, hosted in Amazon Web Services ("AWS").

Protecting our customers' information is at the core of our Information Security strategy. 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.

Online Audit Confirmation Management System

Confirmation NextGen, part of Thomson Reuters, is an online platform designed to increase efficiency, while providing patented fraud detection or prevention capabilities, in the processing of audit confirmations.

Confirmation NextGen provides independent, third party validated, electronic confirmation requests and responses. This validation process provides authorization and authentication procedures that are designed not only to help requestors and responders detect fraud, but also serve as a deterrent or preventative measure against those hoping to circumvent the audit confirmation process.

Why Cloud?

Thomson Reuters' Confirmation NextGen implemented in AWS provides a flexible, reliable, scalable, and secure cloud computing environment with among the highest quality global network performance available. Spanning 4 geographic regions around the world, use of AWS cloud technology provides key redundancy safeguards.

See more on the AWS Global Infrastructure here: https://aws.amazon.com/about-aws/global-infrastructure

Thomson Reuters and AWS Public Cloud Partnership

- Thomson Reuters' AWS solutions follow a shared responsibility model for security, meaning that AWS is generally responsible for the security of the cloud infrastructure and Thomson Reuters is generally responsible for the security of its applications hosted in the cloud.
- Thomson Reuters is part of the AWS Partner Network (APN) which provides multiple resources for customer support, technical training or implementations, and business enablement.
- Thomson Reuters' comprehensive security framework in AWS makes use of selected AWS tools as appropriate to the product and data, which may include:
  - **AWS Guard Duty** monitors for malicious or unauthorized behavior.
  - **AWS Shield Advance** provides protection against Distributed Denial of Service (DDoS) attacks.
  - Network traffic is secure and isolated using AWS Virtual Private Cloud (VPCs), Public/Private subnets, Network Access Control Lists (NACLs), and security groups.
  - **AWS Web Application Firewall** helps protect against common web exploits.
  - **AWS CloudTrail** enables the tracking and analysis of events associated with privileged accounts.
  - Logging, monitoring, and alerting are implemented to assist in the detection of unauthorized use and to produce an audit trail.

Amazon Web Services – Shared Responsibility

Physical and Environmental Security

- AWS secure data centers maintain a diverse set of physical and environmental security controls, including but not limited to:
  - Nondescript facilities
  - Restricted and controlled physical access
  - Professional security staff
  - Video surveillance
  - Intrusion detection systems
  - Authorized staff must pass two-factor authentication a minimum of two times to access data center floors

- AWS data centers are built with electrical power systems designed to be fully redundant and maintainable without impact to operations and include automatic fire detection and suppression.
- AWS monitors electrical, mechanical and life support systems and equipment so that any issues are immediately identified.
- AWS certifications include ISO/IEC 9001:2015, ISO/IEC 27001:2013, and SOC 1, SOC 2, and SOC 3.
- See AWS SOC 3 report here: https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf
- See AWS Security White Paper for more details: https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/introduction-aws-security.pdf

Thomson Reuters – Shared Responsibility

Policies and Standards

- Thomson Reuters manages a set of information security policies and standards that outline information security risk management principles applicable to our people, processes, and technology practices.
- 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).
- Information security policies and standards are reviewed and approved by senior management annually.
- Employees and contractors are required to review and acknowledge the Information Security Handbook.
- Employees and contractors are required to review and acknowledge the Code of Business Conduct Ethics.

Access Control

- Thomson Reuters restricts employee access to production systems and customer stored data by limiting access to those with a specific business need.
- Thomson Reuters uses role-based access controls to implement a least privilege access model to the hosting environment.
- Product authorization controls limit end-user access to customer data.
- Multi-factor Authentication (MFA) supported for customer access using voice, email, or SMS.

Resilience

- Thomson Reuters has established a global, structured framework based on industry accepted standards which are designed to support recovery should a disruptive incident occur.
- Thomson Reuters replicates customer data across geo-distant AWS regions as part of its disaster recovery architecture standards.
- Thomson Reuters' solutions deployed to an AWS region consist of multiple Availability Zones. Each Availability Zone is designed as an independent failure zone. Data is replicated between Availability Zones for high availability and is continuously mirrored to datacenter locations with the four following AWS regions:
  - US East (Northern Virginia) Region (Primary)
  - US West (Oregon) Region (Disaster Recovery)
  - Europe (Ireland) Region (Primary)
  - Europe (Frankfurt) Region (Disaster Recovery)
- Customer data is backed up daily.
- A comprehensive Disaster Recovery Plan has been developed and is routinely tested.
- **AWS Well-Architected Tool** is utilized to integrate architectural best practices designed to achieve secure, high-performing, resilient, and efficient application infrastructure.

Application Security and Vulnerability Assessments

- Thomson Reuters has a formal change management process that is performed by authorized personnel.
- Thomson Reuters incorporates security reviews within the agile methodology as part of the Software Development Life Cycle.
- The application is tested to evaluate availability and security.
- Vulnerability scans are conducted daily on production infrastructure.
- Manual Penetration Tests (MPTs) are routinely performed on the entire platform.
- Application code is regularly scanned by third-party security tools and according to Thomson Reuters policy.

Secure Authentication

- Login credentials to Thomson Reuters systems require a unique identifier and password which must follow password authentication standards.
- All data in transit (from the browser to the server) is encrypted and sent over supported TLS protocols.

Endpoint Security

Servers

- Advanced anti-malware, network intrusion detection system and intrusion prevention system solutions have been deployed across our fleet of devices to monitor and defend the environment by a team of experienced security professionals.

Employee Workstations

- Managed internal services endpoints at Thomson Reuters are protected by an up-to-date version of the standard malware protection solution.
- Automatic anti-virus signature checks and updates run daily.
- Thomson Reuters has a data leakage protection program in place, subject to local law and regulations and where legally permissible.
- Passwords are stored one-way hashed.
- SAML-based Single-Sign On (SSO) is available.

Data Privacy and Compliance

- Thomson Reuters Privacy Statement can be found online: https://www.thomsonreuters.com/en/privacystatement.html
- The Confirmation NextGen platform undergoes an annual SOC 2 examination by an independent third-party auditor.
- All credit card transactions are processed in a PCI-DSS compliant environment.

Training and Awareness

- Employees and contractors with access to Thomson Reuters' systems are required to complete security awareness training annually.
- Thomson Reuters partners with third-party vendors to provide training resources to all skill levels which is tailored to Thomson Reuters Cloud implementations.
- Development staff participates in a security learning program promoting secure design, development, testing, and security industry best practices.

For more information, contact your Thomson Reuters representative.