Online Solutions Security Overview (CORE)

Control Risks ("we") provides Online Solutions for our clients ("you"). Our Online Solutions encompass CORE and CORE+. They provide incisive analysis and forecasting on geopolitical and security issues, a series of country risk ratings and an extensive database of incidents. Coupled with visualisation and analytics tools, these help you make informed business decisions and plan operations in confidence.

This document explains what information we hold and how we secure the information.

The information we hold about your users

Personal data is collected direct from a data subject when they create their own profile and account for the purpose of accessing Online Solutions content through the website or mobile application.

Further information re the types of personal information collected can be found in our GDPR Narrative document in the Trust Centre which also contains a data flow diagram for the CORE service: https://www.controlrisks.com/legal-1/trust-centre

Login process

Our preferred method for your users to log in to CORE services is to use Single Sign-On. We implement SSO (Single Sign-On) using SAML version 2 (Security Assertion Markup Language). In simple terms, it works as follows:

- When a user attempts to log on to our service, the user's browser session is redirected to your domain to be authenticated.
- If the user is not already logged on to your domain in that browser instance, your authentication service will prompt them to log on by their usual method.
- If successful, or if already logged on, your domain will send back a secure message which the browser then passes to our online systems, to confirm that the user in question has authenticated. We ONLY see the user's email address as a default, although you can optionally also include first name and last name in the response message if you choose to.

Note: In single sign-on, we do not have internal access to your network or directory service. We do not extract a list of valid usernames or email addresses – we only receive an email address when a user logs in successfully. The user's password is NEVER visible to our systems.

We also support hosting accounts for your users within the CORE service. Accounts that are hosted within the CORE service enforce strong passwords (better than 8-character with complexity), and lockouts after repeated failed attempts to log in.

How we secure your information

Our strong set of security measures covers the people, process and technology required to assure the confidentiality, integrity and availability of information. It includes policies; screening and training of our people; defined and audited processes; and extensive technological controls such as encryption, segmented data stores, data backups, firewalls, network and communication security, two-factor authentication, and continuous monitoring.

We have an Information Security Management System (ISMS) run from head office, audited and certified to ISO 27001 by BSI. This ISMS includes analysis of risks and legislative requirements, and assessment and implementation of appropriate mitigations on an ongoing basis.

Further information can be found in our Trust Centre https://www.controlrisks.com/legal-1/trust-centre

Hosting

- Our Online Solutions are hosted in Microsoft Azure Europe, which is certified to ISO 27001 and ISO 27018. These establish adherence to strict security controls and procedures. Microsoft Azure staff are security-screened as standard. Further information on Microsoft Azure security is available at: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27018.
- We manage our Online Solutions in Azure through a private cloud. The CORE infrastructure is segregated from other Control Risks services – internal and external. From this perspective the service is self-contained.
- Physical access to the data centre locations by tenants is not permitted. Only Microsoft data centre technicians are able to access the data halls where the infrastructure is located. Access to physical datacentre facilities is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multifactor access control, integrated alarm systems, and around-the-clock video surveillance by the operations centre. Premises are also

Online Solutions Security Overview (CORE)

protected by fire alarms and fire suppression systems.

Infrastructure and security

- Online Solutions have various technologies to protect the services, such as web application firewalls, DDOS protection, malware protection and monitoring agents.
- Online Solutions are only hosted over HTTPS providing end-to-end encryption in transit between the client browser or mobile application and the Online application service.
- All components of the Online Solutions are encrypted at rest.
- Online Solutions are penetration/vulnerability tested at regular intervals by third-party testing companies that are CREST accredited.
- Security patches are applied on a regular defined schedule each month ensuring that the latest vendor security patches are implemented.
- Out of band ("OOB") security patches that are released outside of vendors' normal release schedule is assessed and applied as required.
- Software changes are peer-reviewed. Software and configuration changes go through a formal CAB (change advisory board) process before being deployed.
- Remote management access to the Online Solutions infrastructure is restricted to a defined list of employees, each with individual access accounts audited on a regular basis. No use of generic access accounts is permitted. Account passwords are reset on a regular scheduled basis.
- All components of the Online Solutions are high availability, providing redundancy at all layers in the event of individual service/system failures.

Access controls - your end users

- Access control for your employees is explained in the Login Process section above.
- Access is at two possible levels
  - **End-user** – All users can access to view content and edit their profile information and alert settings.
  - **Account Administrator** – End-user access plus can add users to their allocated account and assign or unassign subscriptions. Account admins can upload and delete asset information and publish incident data. Account admins can also edit profiles and email alerts for users on their account. User deletion is managed by Control Risks administrators.

Access controls - our users

- Access control for our own employees is via Single Sign-On to our directory service with Multi Factor Authentication (MFA) which allows for central control and management. Access is at four possible levels:
  - **End-user** – All Control Risks employees have this access by default, to enable them to access our own research. This level gives them the same access as your users, but not to any of your data.
  - **Administrator** – Can manage End-users and their profiles across all clients.
  - **Editor** – Can add/modify/delete the content (our research).
  - **System Manager** – Can manage the infrastructure and application services.
- Our directory service enforces strong passwords (better than 14-character), and lockouts after repeated failed attempts to log in.

Client defined data: Asset Visualisation / My Incidents

The Asset Visualisation & My Incidents module includes functionality to upload client-specific asset or incident information in bulk.

- Upload files are in Microsoft Excel format (.XLS and .XLSX), thus creating potential threat from the introduction of files – for example – that contain malicious macro context. This threat has been mitigated in the following ways:
  - Client files are not actually uploaded into the Online application. The data is extracted from the file within the browser on the client PC and only the data is transferred. At no time is the actual client file uploaded on to the Online application.
  - The client defined data goes through a series of filters for field checking and validation to ensure that the data is well structured and conforms to required standards, thus ensuring that malicious code cannot be inserted.
- The client defined data is located on servers that are segregated and not publicly accessible. The only access to the data is via an application service that queries the asset data based upon the security of the client logon.
- Client defined data is stored in client-specific data stores referenced by individual client ID providing clear separation between the data of different clients.
- At no point is the individual client ID exposed within browser URLs.

If you have any further questions with regards to the security of our Online Solutions, please do not hesitate to contact your Control Risks' account manager or reach out to us at OnlineSolutions@controlrisks.com.