Online Solutions Security Overview

This document provides an overview of the steps that Control Risks has taken to ensure the security of our online services ("Online"). It does not reference our data centre provider or the location of data centres or make any references to specific vendors, technologies, products or services because this is information that should not be publicly available.

Data Centre and infrastructure

- Control Risks' Online infrastructure is hosted in a UK-based external colocation data centre. This is managed through a private cloud with Online services hosted on infrastructure dedicated to Control Risks.
- The data centre provider is a specialist hosting company, which (among other accreditations) is ISO 27001 and PCI DSS accredited as a service provider. This accreditation establishes adherence to strict security controls and procedures. The data centre's managed services staff are security-screened as standard.
- The Online infrastructure is segregated from other Control Risks services – internal and external. From this perspective the service is entirely self-contained.
- Physical access to the data centre location by clients is not permitted. Only data centre technicians can access the data halls where the physical infrastructure is located.
- The architecture of our Online service is structured so that the infrastructure components are segregated and isolated from each other with only explicit connectivity as required by the applications between the tiers. www.controlrisks.com
- Remote management access to the Control Risks infrastructure is restricted to a defined list of Control Risks' 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.
- The production and pre-production services are hosted within this location and are segregated from each other.

The Online infrastructure and application services are protected by the following technologies as standard:

- Firewalls, with audited rule sets.
- Web Application Firewalls (WAFs) provide additional protection at the application layer.
- Hardware load balancers.
- On-access anti-virus scanners on all infrastructure servers.

Application:

- Control Risks' Online services are only hosted over HTTPS sessions providing end-to-end encryption between the client browser and application service. No Online application services are provided to clients over unencrypted HTTP sessions.
- Online infrastructure services and applications 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.
- Requests for access to the application follow the same approval process regardless if they are external clients or internal Control Risks' employees, ensuring that the same security measures are in place and cannot be bypassed.

Client defined data: Asset Visualisation / My Incidents:

- Asset Visualisation and My Incidents introduces new functionality to the CORE subscription service, where clients are able to bulk upload or individually add client specific asset/incident information into the system.
- Upload files are in Microsoft Excel format (.XLS and .XLSX), thus creating a 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 CORE application or to the CORE infrastructure servers. The data is extracted from the file within the browser on the client PC and **only** the data is transferred to the Online application. At no time is the actual client file uploaded on to the Online service servers.
  - The client 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 asset data is located on servers that are not publicly accessible in any way. The only access to the data is via an application service that queries the asset / incident data based upon the security of the client logon.
- Client asset and incident data is stored in client-specific data stores referenced by individual client ID providing separation between client data.
- 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 services, please do not hesitate to contact your Control Risks' account manager or reach out to us at OnlineSolutions@controlrisks.com.