MyControlRisks – Security Protocol

Control Risks (“we”) provides online solutions for our clients (“you”). Our online solutions include the MyControlRisks platform. MyControlRisks provides secure access to consulting projects from across Control Risks, comprising real-time, data driven dashboards, reports, and analysis product. Access to all content is secured to authorised individuals within the Client and Control Risks organisations. MyControlRisks also provides a channel to raise Experts requests where appropriate to call on the full breadth of experience and capabilities across Control Risks.

User access to the MyControlRisks is protected by multi-factor authentication, and all access is monitored and audited. 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 their account is created for the purpose of accessing MyControlRisks.

Data provided by the data subject will include:

- First Name (mandatory)
- Last Name (mandatory)
- Business Email Address (mandatory)
- Company Name
- Location

Login process

Users are required to log in to MyControlRisks using their business email address, user defined password, and authorisation code from the Microsoft Authenticator MFA application.

User defined passwords must meet complexity requirements and consist of 14–64 characters, including Number, Upper/Lower case, Special characters.

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. This 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 for privileged access, and continuous monitoring.

MyControlRisks undergoes 3rd party penetration testing annually, and sanitised reports can be made available upon request, subject to NDA signature.

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 MyControlRisks 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 can access the data halls where the infrastructure is located. Access to physical datacentre facilities is protected 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 protected by fire alarms and fire suppression systems.

MyControlRisks – Security Protocol

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 client data within 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 are 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.

Access controls – your end users

As explained in the Login Process section above.

- Each user is assigned a username (which must be a business email address). New users receive a registration email which contains a unique link through which they can set a password.
- The link is valid for 14 days. A new link can be sent upon request.
- Current password restrictions are minimum of 14 characters. We cannot see or change the password.
- Users have access to a password reset function via the login page. If a recognised email address is provided, a secure password reset link is sent to that email address.

Access controls

MyControlRisks Users – Client

- User access to all projects, reports and dashboards is by named individual within the client. There is no concept of administrative or elevated access across all content.
- User activity is audited and logged for security monitoring and management purposes.

MyControlRisks Users – Control Risks

- Only Control Risks' staff in client facing roles have access to MyControlRisks in order to demonstrate the functionality to clients/prospects.
- Internal users are setup in the same way as external users. That is, they receive a registration link and then set their own password.
- Internal users only have access to a demo organisation, and client projects authorised by account teams. The same access controls manage Control Risks users as client users – there is no elevated privilege for Control Risks staff.

MyControlRisks Administrators

- The administration of MyControlRisks users, projects, and content takes place within an internal management application. Access to this application is limited to named individuals, and only accessible from the protected Control Risks corporate network.
- Access to the management application is via SSO with our corporate directory service, our directory service enforces strong passwords (better than 14-character with complexity), and locks out after repeated failed attempts to log in.

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 clientsupport@controlrisks.com.