# Information Security

## About Control Risks

Control Risks believes that a strong business reputation depends on a robust data protection and information security program. We view data protection and information security as fundamental components of doing business. Control Risks is committed to protecting information assets, personal data and client information. We believe that solid data protection and information security programs are the essential components of a leading professional services organization. The purpose of this document is to summarize the Control Risks approach to data protection and information security. It provides an overview of how we secure client information and Control Risks information systems that support it. The specifics of these measures may vary depending on the services performed and applicable country regulatory requirements. Control Risks data protection and information security programs and practices are focused on sharing information appropriately and lawfully while preserving confidentiality, integrity and availability.

### Introduction

Information is critical to Control Risks and all our clients and is therefore its protection is a key priority. We host hundreds of thousands of individual records worldwide. The security of this information is of the utmost importance and we continually make sizeable investments to protect our information, IT systems, applications, infrastructure, and processes.

Digital networks are a key enabler in the expansion of our business. They dramatically enhance our ability to communicate, share and store information, and engage with colleagues and clients. New technologies bring new capabilities and, with new capabilities, an increased risk of uncontrolled data disclosure, modification, or unavailability.

At Control Risks, we believe that a strong reputation depends on a robust information security and business resilience programme.

The purpose of this document is to summarise our approach to information security and business resilience. It provides an overview of how we secure client information and our systems housing this information, keeping in mind that the specifics of these measures may vary depending on the service and the applicable country regulatory requirements.

Our information security and business resilience programme and practices are focused on sharing information appropriately and lawfully, while maintaining confidentiality, integrity, and availability.

### Our Approach to Information Security and Business Resilience

Control Risks has developed and implemented a comprehensive information security and business resilience framework aligned to industry best practices such as ISO/IEC 27001:2013 the International Standard for Information Security Management System (“ISMS”), IT Infrastructure Library (“ITIL”) for IT Service Management, and ISO22301:2012 for Business Continuity Management Systems (“BCMS”).

We are certified to ISO/IEC 27001:2013, this certification covers our Group Head office in London. The certificate is available via our website.

Control Risks takes a multi-layered, defence-in-depth approach to protecting the data Control Risks has responsibility for; this includes physical, procedural, personnel and technical security to protect the confidentiality, integrity and availability of its information and services.

This framework and its underlying controls are designed to ensure that:

- Control Risks’ information and systems are only available to authorised people with a justified business need.
- Control Risks’ information is not disclosed or modified without authorisation.
- Control Risks’ information is available when required by relevant business processes; Applicable regulatory, legislative and client requirements are met.
- Information security training and awareness is available for all employees.
- Breaches of security and suspected weaknesses are reported, investigated, documented and resolved.
- Employees have access to clear standards and guidelines that enabled the right attitudes and behaviours; and
- Our brand and financial position are protected from the damage that information security breaches can cause.

Control Risks is committed to maintaining the required secure and resilient infrastructure and architecture to meet its requirements and those defined by our clients, industry, regulatory and legislative standards.

### Information Security and Business Resilience Governance and Policies

The Control Risks Executive Committee ("ExCo") provides top level commitment and support to information security and business resilience across the company.

Information security and business resilience is overseen by the Control Risks' Information Security Forum ("CR-ISF") that reports to ExCo. They oversee information security projects, reports, objectives, and key performance indicators. This group has representation from Control Risks Information Technology, Human Resources, Compliance, Legal, Risk and our business divisions.

Control Risks Group Head office is certified to ISO 27001. All Group policies and standards are aligned to ISO/IEC 27001:2013 and are adopted by all Control Risks business units in all locations. They are owned by CR-ISF and reviewed by key stakeholders across the business.

The Information Security Policy and Standards and Business Continuity Framework is reviewed on an annual basis to reflect any significant changes in Control Risks' structure, business functions and the regulatory environment; or in response to new and emerging threats.

Our Information Security Policy and Standards are communicated to all employees through an information security training and awareness programme and are published via the dedicated information security section of the Control Risks' intranet.

### Human Resource Security

All Control Risks employees are subject to screening prior to employment. The screening process is conducted in accordance with relevant national laws and industry regulations and provides verification of identity and credentials, as well as evaluating applicant integrity.

All Control Risks employees are subject to confidentiality/non-disclosure agreements as part of the standard employment contracts and are required to comply with the controls outlined in the Information Security Policy and Standards, including Acceptable Use of ICT Policy. All employees acknowledge that they have access to and have read this documentation annually.

The CR-ISF oversees the information security training and awareness programmes to ensure that all employees are aware of their responsibilities and have the necessary resources to maintain our position on information security.

These programmes include mandatory annual online training for all employees; targeted security campaigns that cover specific issues such as simulated phishing exercises and more detailed technical security training for the Control Risks technology teams such as secure software development.

When an employer leaves, Control Risks applies robust procedures to ensure the timely removal of access rights to IT systems as well as the retrieval of any physical information assets which are recorded in the asset inventories.

### Asset Management

Control Risks has implemented an information classification scheme for all information that supports its day to day business activities. Control Risks maintains inventories of its information assets, including applications and IT systems.

Control Risks uses enterprise solutions to create and maintain an inventory its assets. The Acceptable Use Standard details the acceptable use by staff of those assets.

The Asset Classification and Handling Standard requires all client information to be classified and handled as CONFIDENTIAL or above.

Data Loss Prevention ("**DLP**") software is deployed across the entire estate. All user endpoints by default to DENY for removable media (e.g. USB, CD/DVD, mass storage devices).

Local certified companies are used for secure destruction for paper and magnetic media. The default destruction method for all assets containing information is physical destruction. Certificates of destruction are required and retained.

### Physical and Environmental Security

All Control Risks office locations operate risk-based controls to provide protection against unauthorised physical access. These include physical and electronic access control systems, manned reception desks, CCTV and security lighting.

Access to our data centre facilities and other information processing locations is strictly controlled and restricted to pre-authorised individuals only. This access is logged, and the access rights are reviewed on a regular basis.

All Control Risks data centre facilities are ISO27001 certified and are rated Tier 3 or above, which provides a high level of redundancy, physical security and environmental control including fire detection and prevention, dual power supplies, monitored Uninterruptable Power Supply ("UPS"), back-up generators, temperature, smoke, water and humidity controls.

### Access Control

Control Risks operates on the principle of 'least privilege' for access control. This is to ensure that only authorised individuals are permitted access to our business applications, systems, networks and computing devices; that individual accountability is established and to provide authorised users with the access permissions that are sufficient to enable them to perform their duties but do not permit them to exceed their authority. Access is provided under Role Based Access Control ("RBAC") and activity is logged and monitored.

Access is co-ordinated through the IT Service Desk and all access requests must be authorised by an employee's line manager and/or the assigned resource owner. There are regular reviews of user access rights to detect and remove any inactive accounts and inappropriate access permissions.

All Control Risks employees are assigned unique user IDs and are required to select and manage their passwords in line with our Password Standard. In the event of a change of employment status or role, user access rights are immediately revoked or reassigned by the relevant regional IT Service Desk upon notification from the line manager.

The use of privileged accounts is strictly controlled and restricted to system administration and maintenance activities only. Additional measures are employed to securely manage these accounts. This includes enhanced password management controls such as a more complex structure requirement and increased change frequency.

Remote access to the Control Risks network is only permitted for pre-authorised employees using a Control Risks' managed asset. This is achieved using an encrypted VPN solution and is supported by multi-factor authentication.

#### Cryptography

Control Risks services use internally approved cryptographic algorithms and processes that conform to industry standards for encryption and key management.

All Control Risks desktops and laptops have full disk encryption using AES256. All back-end mass storage is encrypted-at-rest using AES256. All back-up tapes are encrypted using AES256. Exchanges of confidential information across untrusted networks are encrypted-in-transit using TLS or IPSEC.

#### Communications and Operations Security

Control Risks has implemented a defence-in-depth approach to protect its information and IT systems from existing and emerging threats. The management and operation of our IT systems is delivered by our highly experienced technology teams using a service management model based upon the Information Technology Infrastructure Library ("ITIL") standard. This includes the formalisation of processes and procedures to support core activities such as back-up and recovery, change management, release management and capacity planning.

Control Risks has a disaster tolerant network and computing architecture design across all its global data centres. Where appropriate our multi-tier internet-facing infrastructure uses two physical layers of firewalls supporting three-tier application deployment and secure segregation of different networks, connections, and systems. Server virtualisation provides rapid resource provisioning and enhanced failover and disaster recovery capabilities.

All Control Risks IT systems are configured following technical security standards which include applicable controls such as system hardening, encryption, anti-virus and data loss prevention and regular patching. The CR-ISF actively monitors security key performance indicators and works with the relevant teams to ensure that the current security controls deployed are both appropriate and effective, to mitigate risk.

The Control Risks' IT technical security controls are monitored by a security operations centre which collects and correlates the event logs from network devices, firewalls, IDS and web application firewalls. This data is analysed and any unusual or suspicious events generate the necessary alerts which are handled by our information security incident management processes.

### System Acquisition, Development and Maintenance

Control Risks follows a defined System Development Life Cycle ("SDLC") that incorporates information security throughout each stage including risk assessments, the identification and implementation of control requirements, static and dynamic code analysis and technical security penetration testing.

Control Risks maintains separate development, test and production environments and has strict policies to enforce segregation of duties for employees responsible for development, testing and support activities. Our source code, including all applications under development, are stored and protected in an approved source code system with audit logging enabled to track activity such as code modification and deletion.

### Supplier Relationships

Control Risks' supply chain assurance program covers third party activities which are audited based on risk for information security and business resilience. This may include the evaluation of prospective vendors for compliance with Control Risks ISO27001/2 aligned Information Security Policy and Standards, risk identification, rating and finding management, contract review including confidentiality clauses, the right to audit and detailed contractual security requirements where required.

### Information Security Incident Management

Control Risks has global risk-based processes to respond to information security incidents, unusual or suspicious events and breaches of policies. These processes are owned and coordinated by the Group Information Security manager with formal involvement from relevant stakeholders (e.g. legal, compliance, risk, IT, human resources, , marketing, finance and service lines).

The information security incident management processes are designed to contain and control the incident, reduce any potential impact to the business, identify and investigate the root cause and implement corrective actions to reduce the risk of recurrence. These processes are supported by procedures for identification, reporting, assessment, response, recovery and follow-up. Our post-incident procedures include root cause analysis, forensic investigation and, where required, notification to the relevant authorities and affected clients.

All Control Risks employees are provided with new joiners onboarding training, annual online information security and data privacy training, phishing simulations and guidance to identify and report information security incidents. Periodic Information security communications inform employees of the latest threats and trends.

### Business Continuity Management

Control Risks has an established Business Continuity Management programme that supports our regulatory and contractual requirements.

All Control Risks 'offices, services lines and functions are included within the business continuity management programme and are required to have in place a business continuity plan. Our business continuity plans and disaster recovery plans are developed and maintained by assigned owners from within the business and information technology teams and are regularly updated to reflect any change of circumstances.

Control Risks performs annual tabletop business continuity and disaster recovery tests on a periodic basis to ensure that the plans can be employed should the need arise. Senior management take part in scenario-based Crisis management training annually.

### Audit and Compliance

The CR-ISF oversees and measures compliance with the Information Security Policy and Standards through periodic technical and non-technical control assessments. Our technical control assessments include regular vulnerability scans and annual penetration tests using United Kingdom National Cyber Security Centre CHECK approved testers. Our non-technical control assessments include internal audit, information security management system reviews and security KPIs.

We are externally audited every year to maintain our ISO/IEC 27001:2013 certification. The certificate is available via our website.

The results of these reviews are documented, managed through to remediation, and reported to the CR-ISF monthly.

### Summary

Clients and individuals rightfully demand accountability from any organisation handling their personal and confidential data. We understand the importance of taking appropriate steps to safeguard information and are committed to protecting information relating to our clients and to our people.

We trust this demonstrates the commitment and considerable investment Control Risks has made to information security and that our clients, business partners, employees and wider stakeholders can have full confidence in the confidentiality, integrity and availability of our information and IT systems.

If you have any specific questions or would like additional information on the measures that we take to protect your information, then please contact your nominated Control Risks' relationship manager.