ramco

Protecting your Data on the Cloud
An overview of Ramco's Data Security Measures on the Cloud

Customer Background

This white paper describes how Ramco Systems ensures that customer data is well protected in its data center.

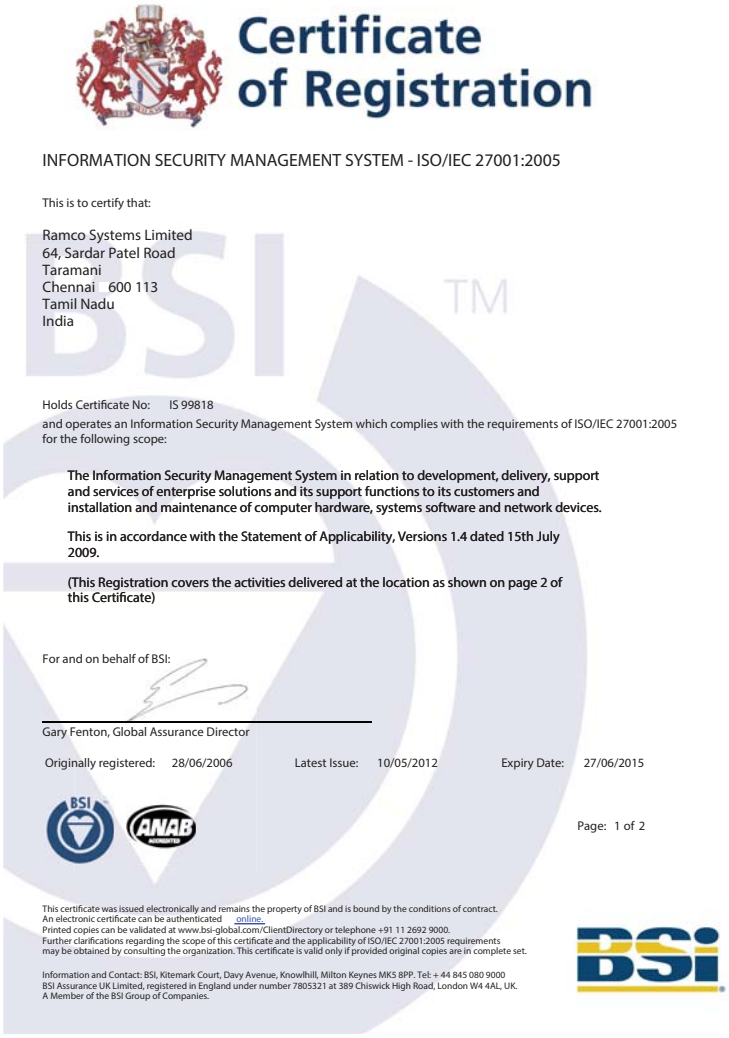
Data generated by companies through their business transactions is vulnerable to security threats, irrespective of whether they are stored within a client's premises or elsewhere in remotely located data centers, managed by third party service providers like Ramco Systems. The real cause for concern when it comes to data security is therefore not so much where the data is located as the clients' perception about the vulnerability of their data.

Firms feel secure about data stored within their own premises, seemingly under their control. The reason is not difficult to understand—data residing elsewhere cannot be "watched" by the customer, and this can create a psychological discomfort. The issue here is really no different from that surrounding our household valuables. Some individuals feel secure about storing their valuables inside their homes, while some others would avail of third party locker facilities. The protection which comes with third party lockers far outweighs the psychological discomfort of not being able to "watch" the storage facility located outside one's home.

Ramco Systems Limited not only secures the data of its own business, but also that of its customers. Data stored in Ramco's data centers tends to be more secure than in a client's premise for several reasons.

The data center in Ramco Systems has more than 430+ servers. These servers hold the worldwide business data of customer projects being executed by Ramco Systems. These servers are also connected to the global offices of Ramco Systems and their customers through high-speed networks and telecommunication systems.

To protect its data, Ramco Systems has put in place a comprehensive Information Security System as mandated by ISO27001 standards. This security system was subject to rigorous audit by BSI of London before certification. The certificate is an authentication of data and Information Security at the data center of Ramco Systems. A copy of the certificate is included.



Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that:

Ramco Systems Limited
64, Sardar Patel Road
Taramani
Chennai 600 113
Tamil Nadu
India

Holds Certificate No: IS 99818

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

The Information Security Management System in relation to development, delivery, support and services of enterprise solutions and its support functions to its customers and installation and maintenance of computer hardware, systems software and network devices.

This is in accordance with the Statement of Applicability, Versions 1.4 dated 15th July 2009.

(This Registration covers the activities delivered at the location as shown on page 2 of this Certificate)

For and on behalf of BSI:

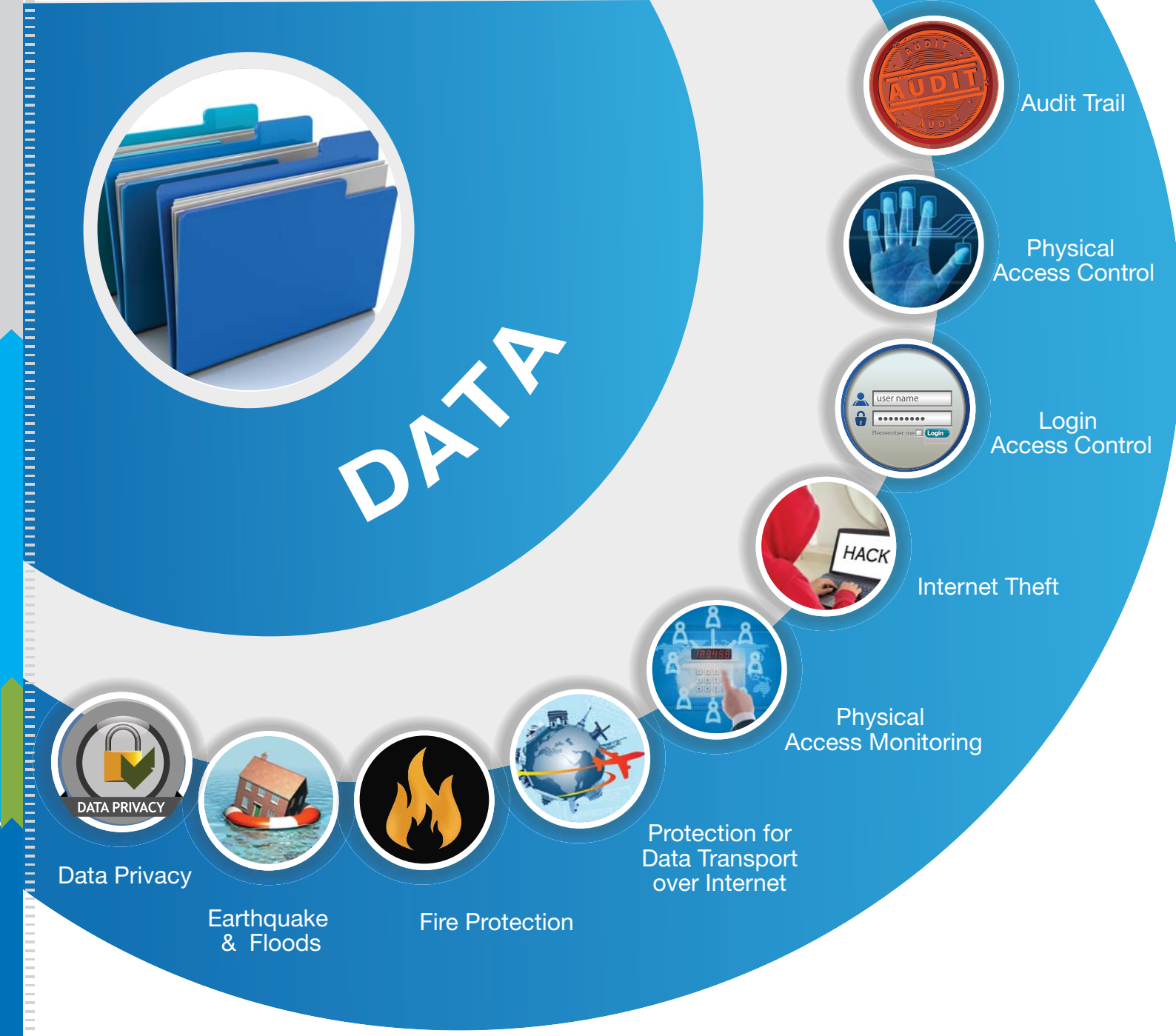
Gary Fenton, Global Assurance Director

Originally registered: 28/06/2006 Latest Issue: 10/05/2012 Expiry Date: 27/06/2015

Page: 1 of 2

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +91 11 2692 9000.
Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27001:2005 requirements may be obtained by consulting the organization. This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 845 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.



Internal Theft: One of the security threats comes from unscrupulous employees. Such employees can pass data to competitors. Locating data in highly secure third-party data centers can deter employees from stealing data. The data center personnel employed by Ramco Systems have their backgrounds verified extensively during the recruitment process. They will not have an understanding of the customers' businesses as much as an internal employee of the customer. So their interest in the data is greatly reduced, thereby mitigating data theft risks.

Physical Access Control: The data center is a sensitive zone. Only authorized personnel can enter it. The entry is controlled through automatic access control systems that are linked to security alarms. This prevents public access and stray entries. All such entries are automatically logged in entry logs.

Physical Access Monitoring: The area in and around the data center is monitored 24X7 through surveillance cameras which capture the images of those entering that area. The video records are archived. Security guards are constantly watching the video monitor.

Login Access Control: This is a two dimensional access control measure. Firstly, only authentic users can login. Secondly, they can login only to the relevant transaction screens for which they have permissions. This mechanism prevents any unauthorized access to both transactions and data. Customers can define the access polices, or it can be set by an administrator designated by the customer. This way, the customer gets absolute control over the access.

Audit Trail: Even authentic usage is constantly tracked to find out who logged in, when the login happened, what the duration of the login was, what the usage pattern is, unusual usages noticed and so on, these are but a few of the possible ways by which tracking happens. Such trails discourage anyone from attempting to misuse the data. Thus, frauds can be both prevented and detected.

Data Transport over Internet: Data movements over the internet from the customers' office(s) to Ramco's data center is protected through encryptions and transported over a secure sockets layer. This prevents theft, as encryption renders the data meaningless and makes any theft harmless.

Firewall: Data arriving through the internet at the data center is filtered through the firewall. This is like immigration control, designed to detect illegal entrants. Only an authentic customer's data finally reaches the servers. Firewall policies are continually updated as per the Information Security Management System implemented in Ramco Systems. This protects customers' data from malicious software attacks.

Privacy: Privacy can be looked at in three ways.

Internal privacy : Here, the data from one department cannot be viewed or altered by another department. For instance, accounts data cannot be accessed by a stores person.

External privacy : This ensures that the customer's data is not available to anybody else. This is established by allocating separate databases for each customer. Also, the servers dedicated to each of the customers, run on separate networks. So traffic from other networks, including that of Ramco employees, cannot access the customer's network.

External privacy involving government and regulatory bodies: This is strictly governed by contractual agreements with the customers. Any request for data belonging to customers will not be entertained without the involvement of the customers.

Fire and Natural Calamities: Natural disasters can happen anytime, anywhere and affect data and business activities. Fire, earthquakes and floods can ruin data and disrupt operations. Ramco has implemented a disaster recovery mechanism to handle such crises. First, the data center itself is subject to fire safety regulations. Second, all data is stored on high speed storage area networks. Data is backed up according to the data backup policy required by the Information Security Systems. Daily, weekly and monthly back-ups are taken. In the case of any unforeseen event, the media containing the back-up is restored for smooth operations to continue.

Conclusion: Ramco Systems takes the business of data security very seriously. Ramco runs its own worldwide business operation out of its data center and consequently appreciates the sensitivity towards data security. Information Security Management Systems (ISMS) is a comprehensive set of policies and procedures designed and implemented to realize very high levels of data and Information Security. This is continually received and accessed for effectiveness. Ramco Systems is fully committed to the security policy. As a mark of this commitment to information security, BSI Management Systems of the BSI Group, UK () recommended the ISO27001 certificate to Ramco Systems.