



CERTIFICATE OF APPROVAL

This is to certify that the Information Security Management System of:

**Ansarada Pty Limited
Sydney, New South Wales
Australia**

has been approved by Lloyd's Register Quality Assurance Limited to the following Information Security Management System Standards:

ISO/IEC 27001:2005

The Information Security Management System is applicable to:

**The provision by Ansarada of information security for client information in virtual datarooms accessible worldwide.
Statement of Applicability 2.0**

Approval
Certificate No: MEL 6006028

Original Approval: 30 June 2009
Current Certificate: 19 October 2009
Certificate Expiry: 30 June 2012

Lynette Srinivas

Issued by: Lloyd's Register Quality Assurance Limited



This document is subject to the provision on the reverse

71 Fenchurch Street, London EC3M 4BS United Kingdom. Registration number 1879370

This approval is carried out in accordance with the LRQA assessment and certification procedures and monitored by LRQA.

The use of the UKAS Accreditation Mark indicates Accreditation in respect of those activities covered by the Accreditation Certificate Number 001

To confirm the validity of the accreditation for this certificate please visit www.jas-anz.com.au/register

Macro Revision 13



The Statement of applicability specifies the implementation by Ansarada for its data room service of the controls contained in ISO Standard 27001 Security Techniques Information Security Management Systems. Listed below are controls which are applicable to Ansarada's Information Security Management Systems

- A.5.1.1 Information security policy document
- A.5.1.2 Review of the information security policy
- A.6.1.1 Management commitment to information security
- A.6.1.2 Information security coordination
- A.6.1.3 Allocation of information security responsibilities
- A.6.1.4 Authorization process for information processing facilities
- A.6.1.5 Confidentiality agreements
- A.6.1.6 Contact with authorities
- A.6.1.7 Contact with special interest groups
- A.6.1.8 Independent review of information security
- A.6.2.1 Identification of risks related to external parties
- A.6.2.2 Addressing security when dealing with customers
- A.6.2.3 Addressing security in third party agreements
- A.7.1.1 Inventory of assets
- A.7.1.2 Ownership of assets
- A.7.1.3 Acceptable use of assets
- A.7.2.1 Classification guidelines
- A.7.2.2 Information labelling and handling
- A.8.1.1 Roles and responsibilities
- A.8.1.2 Screening
- A.8.1.3 Terms and conditions of employment
- A.8.2.1 Management responsibilities
- A.8.2.2 Information security awareness, education and training
- A.8.2.3 Disciplinary process
- A.8.3.1 Termination responsibilities
- A.8.3.2 Return of assets
- A.8.3.3 Removal of access rights
- A.9.1.1 Physical security perimeter
- A.9.1.2 Physical entry controls
- A.9.1.3 Securing offices, rooms and facilities
- A.9.1.4 Protecting against external and environmental threats
- A.9.1.5 Working in secure areas
- A.9.1.6 Public access, delivery and loading areas
- A.9.2.1 Equipment sitting and protection
- A.9.2.2 Supporting utilities
- A.9.2.3 Cabling security
- A.9.2.4 Equipment maintenance

A.9.2.5 Security of equipment off premises
A.9.2.6 Secure disposal or re-use of equipment
A.9.2.7 Removal of property
A.10.1.2 Change management
A.10.1.3 Segregation of duties
A.10.1.4 Separation of development, test and operational facilities
A.10.2.1 Service delivery
A.10.2.2 Monitoring and review of third party services
A.10.2.3 Managing changes to third party services
A.10.3.1 Capacity management
A.10.3.2 System acceptance
A.10.4.1 Controls against malicious code
A.10.4.2 Controls against mobile code
A.10.5.1 Information back-up
A.10.6.1 Network controls
A.10.6.2 Security of network services
A.10.7.1 Management of removable media
A.10.7.2 Disposal of media
A.10.7.3 Information handling procedures
A.10.7.4 Security of system documentation
A.10.8.1 Information exchange policies and procedures
A.10.8.2 Exchange agreements
A.10.8.3 Physical media in transit
A.10.8.4 Electronic messaging
A.10.9.3 Publicly available information
A.10.10.1 Audit logging
A.10.10.2 Monitoring system use
A.10.10.3 Protection of log information
A.10.10.4 Administrator and operator logs
A.10.10.5 Fault logging
A.10.10.6 Clock synchronization
A.11.1.1 Access control policy
A.11.2.1 User registration
A.11.2.2 Privilege management
A.11.2.3 User password management
A.11.2.4 Review of user access rights
A.11.3.1 Password use
A.11.3.2 Unattended user equipment
A.11.3.3 Clear desk and clear screen policy
A.11.4.1 Policy on use of network services
A.11.4.2 User authentication for external connections
A.11.4.3 Equipment identification in networks
A.11.4.4 Remote diagnostic and configuration port protection
A.11.4.5 Segregation in networks
A.11.4.6 Network connection control
A.11.4.7 Network routing control

- A.11.5.1 Secure log-on procedures
- A.11.5.2 User identification and authentication
- A.11.5.3 Password management system
- A.11.5.4 Use of system utilities
- A.11.5.5 Session time-out
- A.11.6.1 Information access restriction
- A.11.6.2 Sensitive system isolation
- A.11.7.1 Mobile computing and communications
- A.11.7.2 Teleworking
- A.12.1.1 Security requirements analysis and specification
- A.12.2.1 Input data validation
- A.12.2.2 Control of internal processing
- A.12.2.3 Message integrity
- A.12.2.4 Output data validation
- A.12.3.1 Policy on the use of cryptographic controls
- A.12.3.2 Key management
- A.12.4.1 Control of operational software
- A.12.4.2 Protection of system test data
- A.12.4.3 Access control to program source code
- A.12.5.1 Change control procedures
- A.12.5.2 Technical review of applications after operating system changes
- A.12.5.3 Restrictions on changes to software packages
- A.12.5.4 Information leakage
- A.12.6.1 Control of technical vulnerabilities
- A.13.1.1 Reporting information security events
- A.13.1.2 Reporting security weaknesses
- A.13.2.1 Responsibilities and procedures
- A.13.2.2 Learning from information security incidents
- A.13.2.3 Collection of evidence
- A.14.1.1 Including information security in the business continuity management process
- A.14.1.2 Business continuity and risk assessment
- A.14.1.3 Developing and implementing continuity plans including information security
- A.14.1.5 Testing, maintaining and reassessing business continuity plans
- A.15.1.1 Identification of applicable legislation
- A.15.1.2 Intellectual property rights (IPR)
- A.15.1.3 Protection of organizational records
- A.15.1.4 Data protection and privacy of personal information
- A.15.1.5 Prevention of misuse of information processing Facilities
- A.15.1.6 Regulation of cryptographic controls
- A.15.2.1 Compliance with security policies and standards
- A.15.2.2 Technical compliance checking
- A.15.3.1 Information systems audit controls
- A.15.3.2 Protection of information systems audit tools