Australian Securitisation Forum

3 Spring Street, Sydney NSW 2000

www.securitisation.com.au

LOAN LEVEL DATA DISCLOSURE

Due diligence guidance notes for sponsors

1. Due diligence approach and coordination

The level of due diligence required may vary from sponsor to sponsor depending, in part, on the risks assessed to be associated with the applicant seeking access to the loan level data.

Privacy risks are likely to be higher for users with less sophisticated and less well-established practices, procedures and systems for handling personal and/or sensitive information.

Schedule 1 - User Information to the ASF Pro-forma "ASF Data Access Deed – RMBS" requires basic information about the applicant, their purpose for seeking access to the loan level data and information to assist highlight privacy risk factors. Certain applicant responses to Schedule 1 to the ASF Data Access Deed – RMBS indicate higher privacy risk factors. In these circumstances, additional due diligence is recommended to ensure that appropriate safeguards are in place to minimise any impact on individuals' privacy.

2. Due diligence guidance notes

The Due Diligence Guidance Notes for sponsors that follow provide reference materials for sponsors to assist them to further assess the risks associated with the applicant seeking access to the loan level data and safeguards to minimise any impact on individuals' privacy. For certain higher risk applicants, it may be appropriate to complete all the due diligence measures outlined in the Due Diligence Guidance Notes.

3. Due diligence information

Description	Requirements
Applicant organisational structure	Review copies of the following information: a. Name of the holding or parent company (if any) b. Publicly or privately held company

Description	Requirements
	c. Most recent financial statements d. Organisational structure chart e. Number of employees f. Applicable regulators g. Company website URL h. Brief company history i. Licences held j. Auditors k. Details of professional indemnity insurance policies including limits and coverage
Applicant qualification	Please provide details of your organisation's qualification under the nominated Permitted User category: a. Amount previously invested in RMBS and proposed future investments in RMBS b. Number of investors subscribing to or receiving research published on RMBS, and their estimated RMBS funds under management c. Details of market data platform provided or, and current number of RMBS data contributors on market data platform d. Number of cashflow-modelled RMBS transactions and number of issuers covered e. Government, regulator or central bank function and relationship to RMBS securitisation f. Number of Australian RMBS transactions for which your organisation provides a credit rating g. Details of the entity for which your organisation is a representative h. Details of your status as a market professional for RMBS securitisation and proposed future investment in RMBS i. Details of academic research platform provided and number of academic organisations utilising research platform j. Details of historical experience in managing data sets containing information of a sensitive nature

Description	Requirements
Staff access to data	Please provide details of the staff or teams within your organisation who will be granted access to the data, including; a. What teams/departments within the organisation will have access to the data? b. How many staff are in each team/department? c. Have the individuals within each team/department been subject to probity checks? d. Employee name e. Email address f. Work address g. Phone number h. Functional role i. Length of service j. Employee Username on *ABSPerpetual* or other secure website for provision of data
Infrastructure security	Please provide details of your organisation's infrastructure security, including: a. Do you have a network topology diagram relevant to the service being offered? If yes, please provide a copy. b. How is multi-tenant-owned or -managed (physical and virtual) applications, and infrastructure system and network components, designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users? c. Are internet accessible systems deployed in a DMZ network? d. Are stateful inspection firewalls used to isolate network segments? e. If this is a web based system or application, do you have a web application firewall protecting the application from attacks? f. Are Standard Operating Environments used for your server and application builds? g. Is hardening of network devices, operating systems, database, and web/application servers performed? If yes, please share guidelines/standards or practices you follow. h. What secure and encrypted communication channels are used when migrating physical servers, applications, or data to virtualized servers? i. Is access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems restricted to personnel based upon the principle of least privilege?

Description	Requirements
	j. If so, how? (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles). k. Is the principle of least privilege access used when granting access to hosting infrastructure? l. Do you review user accounts on infrastructure, and close inactive accounts regularly (e.g. every 90 days)? m. Do you provide staff or contractors remote access to your environment? If yes, please provide details on what authentication and other access controls have been implemented. n. Is there a process to remove access rights to terminated employees?
Security policies and procedures	Please provide details of your organisation's security policies and procedures, including: a. Is there a defined role with responsibility for information security within the organisation? If yes, what is / are those roles? b. Do you have an information security program in place that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorised access, disclosure, alteration, and destruction? c. Do your information risk and security policies and standards cover the following: - Information classification - Data handling, including secure usage, storage and destruction of Personally Identifiable Information - Internet and/or intranet access and use - Access control - Acceptable use of corporate computing resources - Email use, handling and storage - Secure transmission and approved standards (e.g. approved encryption, transfer protocols) - Minimum security standards for network devices, operating systems, workstations, servers and applications - Software development life cycle - Change management - Security and privacy incident management - Remote access - Security and privacy training and awareness - Physical security - Business continuity

Description	Requirements
	d. Do these policies have an owner and are they actively maintained? e. How are information risk and security policies communicated to employees? f. How often are user access reviews conducted? g. Does your organisation undertake system penetration testing? If so, how often? h. Will all the Restricted Data be encrypted?
Access management and data protection	Please provide details of your organisation's access management and data protection, including: a. Do all users of the application have individual identities (including administration/support accounts)? b. Does the application support Federated Identity Management authentication such as SAML? c. Does the application support the concept of roles? d. Is the principle of least privilege supportable through the use of roles? e. Can the application allow the delegation of user administration to any third parties? f. Is it possible to get ad hoc reports on users registered for the service? g. Do you use segregation of duties between development teams and production support? h. Does the application support, and do you implement, the following password policies (if configurable, please list the options available)? - Password complexity (use of different character sets e.g. alpha, numeric) - Password ageing - Password history - Minimum password length - Account lockout after a defined set of failed login attempts - Account logout after a defined period of inactivity - 2-factor authentication or IP whitelisting for remote access (if applicable)? i. Does the application have a 'Forgot Password' function? If yes, please explain how this feature works (e.g. self-support for reset, who sets the new password, how is it shared with requestor, is it forced to be changed) j. Does the application support automatic session logout / termination after a configurable period of user inactivity? k. Are user credentials encrypted in transit at all times?

Description	Requirements
	l. If so, what encryption is applied? m. Are user credentials encrypted in storage? If yes, please provide details of how this is done (e.g. what hashing mechanism is used). n. Is the Restricted Data encrypted in storage? If yes, please share nature of encryption and key management. o. This question relates to all storage methods (i.e. filesystem, database, local backups, tape backups) p. How do you securely connect enterprise networks to your hosted service?
Threat and security incident management	Please provide details of your organisation's threat and security incident management, including: a. Do you have a patch management process? If yes, please describe the patching process and frequency of applying patches. b. Do you monitor websites of your vendors/providers (e.g. Oracle, Microsoft) or of third-party software components (e.g. Apache Web Server) for product security alerts? c. Do you have a vulnerability management process? If so, please provide details. d. Describe the policies and controls protecting against malicious software at both the server and client levels of your network. e. Are all systems on the network deployed with up-to-date anti-malware/antivirus software? If yes, please provide details. f. Do you use security monitoring and alerting systems on critical systems/network segments? If yes, please describe the process of how you respond to a security alert. g. Is an actively managed and monitored intrusion prevention/detection system implemented within the network? If yes, how are alerts generated by these systems acted upon? h. Do you currently have protection against denial of service (DoS/DDoS) attacks with respect to the service being offered? i. If yes, please provide details of network and application level DoS protection mechanisms. j. Has the infrastructure hosting the application applications undergone a vulnerability scan conducted by an independent security testing agency or team? If yes, please provide the detailed report for review. k. Do you have security incident / data breach response policies and procedures?

Description	Requirements
	l. Does your organisation have cybersecurity insurance for protection against data breach? m. Have you had any security incidents in the last two years? If so, please provide details. n. What processes are in place to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures? o. Will the RMBS Issuer be notified in the event of a security incident (e.g. Website defacement, Phishing attacks, Denial of Service (DoS/DDoS) attacks etc.)? If yes, please explain the notification process. p. Can audit trails support forensic enquiry and reconstruction of events leading to a system security incident or system failure? q. In the event a follow-up action concerning a person or organisation after an information security incident requires legal action, what forensic procedures, including chain of custody, are in place for the preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction?
Data management	Please provide details of your organisation's data management, including: a. What is your process for managing the data lifecycle - data creation, access, storage, destruction/decommission? b. What procedures are in place for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations? c. Does your organisation have a Data Loss Prevention (DLP) and/or Information Rights Management (IRM) solution implemented? d. What data centre locations are available for storage and processing of customer data? e. Will the Restricted Data be handled or stored on shared computing services, including cloud-based data storage, either self-managed or third party managed? If yes, please provide a description of arrangement? Where will the Restricted Data be stored? f. What assurance can you provide that data will not be relocated without consent? g. What processes are in place for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means? h. Are all servers and network equipment hosted within premises managed by you, or within a co-located data centre? If within a co-located facility, please provide details.

Description	Requirements
	i. Is this service hosted on third party provided infrastructure? (e.g. Rackspace, Amazon) j. Are these data centres physically secured? If yes, please outline the physical security measures which have been implemented (e.g. security cameras, presence of guards, visitor validation). k. Has there been an independent review of the security and environmental controls implemented in these data centres? (e.g. ISO 27001, SOC 1, SOC2, PCI DSS certification). If yes, please provide the latest assessment report. l. Is the customer data environment segmented from the organisation's corporate network? m. Will the Restricted Data instance be physically segmented from other company's data?
Regulatory compliance	Please provide details of your organisation's regulatory compliance, including: a. How do ensure you comply with relevant privacy laws and protect private data collected, stored or processed? b. How is your organisation setup to liaise with applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities to ensure direct compliance liaisons have been established in preparation for a forensic investigation requiring rapid engagement with law enforcement? c. What sort of logging or auditing do you provide for surveillance and discovery purposes? d. How do you comply with data protection requirements relating to data located in multiple jurisdictions? e. What training is undertaken for staff on management of personal information? f. What restrictions will be placed on staff not to match data to identify individuals? g. Will authorised staff's access to real estate sales information databases be removed? h. Do employees sign a document acknowledging their receipt and understanding of user's Information Security policies and Codes of Conduct? i. How often are the policies reviewed, and are employees reminded of their responsibilities in relation to these policies on a regular basis? j. What are the consequences of breach of these policies? k. Is your organisation covered by the Privacy Act 1988 (Cth) (Privacy Act), and if not what exemption applies?

Description	Requirements
	l. If you are not covered by the Privacy Act, will your organisation opt-in to the Privacy Act in relation to the RMBS Issuer and all of the individuals whose data is disclosed in the Restricted Data? m. Will your organisation maintain its opt-in to the Privacy Act, and notify the RMBS Issuer if it proposes to change its opt-in status? n. If you are an overseas entity, are you covered by legislation equivalent to the *Privacy Act*, and if so please advise which legislation this is? o. What internal approval process is the entity undertaking to ensure senior management are aware of and will ensure appropriate systems and resources are employed to maintain security of the Restricted Data?
Governance and risk management	Please provide details of your organisation's governance and risk management, including: a. Is there an enterprise risk assessment framework in place to identify, assess and mitigate risk to an acceptable level? b. How often are organisation wide risk assessments conducted to determine the likelihood and impact of all identified risks? c. What is the process for remediating high and medium risk findings? d. On what basis are risks accepted in the organisation? e. Does your organisation's internal control framework align with any industry recognised standards? (e.g. COBIT, ITIL). If so, please advise. f. What external/internal audits/certification are performed? g. Have any of the above audits resulted in findings or exceptions? - Internal audit findings - External audit findings - Regulatory/legal findings - SOC1 or SOC2 exceptions - ISO 27001 standards compliance
Third party access	Please provide details of your organisation's third party access, including: a. Are there any other third parties who would have access to the Restricted Data or systems hosting the Restricted Data information? (e.g. outsourced developers, external testers, remote sysadmins) b. If yes, please provide details on the third parties and the due diligence undertaken on them.

Description	Requirements
	c. If you subcontract out to other parties do you have full visibility of their operations? d. If you subcontract out to other third parties can you provide evidence that these organisations are compliant with the ASF Data Access Deed requirements for security, risk and relevant regulatory requirements? e. If you outsource and BCP or DR services, do your third-party providers maintain their own Business Continuity and DR plans? f. Are there access mechanisms in the areas of privacy, information security, and disaster recovery (e.g. ongoing risk assessments) as they relate to third parties? g. Do your service agreements with dependent third parties clearly specify all relevant terms, conditions, responsibilities, and liabilities of both parties? (This includes, but is not limited to, such items as audit, protection of confidential information, compliance with policy, compliance with laws and regulations, Business Continuity/Disaster Recovery, insurance, post termination obligations, site access, staffing, and system security requirements) Please provide a sample agreement.
Application security and service features	Please provide details of your organisation's application security and service features, including: a. Is this a web based application? If yes, please provide details of the technology stack for the front end (e.g. .NET or PHP) and backend database (e.g. Oracle or MySQL). If no, please provide details of the technology used. b. Is security factored into different stages of your SDLC? If yes, please provide details of how this is done. c. Do you perform static and/or dynamic source code review from a security perspective? If yes, please provide details. d. What data input and output integrity routines (i.e., reconciliation and edit checks) are in place for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse. e. Does the application support secure integration at transport layer (e.g. SFTP, HTTPS)? If so, please provide details. f. Is the administration (user creation, password reset etc.) performed within the application/system? If not, please provide details where the administration component is hosted and accessed from. g. Is the Restricted Data used within your test or development environment? h. Does the application require data feeds from the RMBS Issuer's systems? If yes, please describe how this data would be transferred between the RMBS Issuer and your network (e.g. FTP, SFTP, web services)

Description	Requirements
	i. Does the application send data feeds to the RMBS Issuer's systems? If yes, please describe how this data would be transferred between your network and the RMBS Issuer (e.g. FTP, SFTP, web services). j. Is the Restricted Data exchanged between one or more system interfaces or jurisdictions outside of the service components used by your organisation? If yes, please describe security controls in place to ensure protection of confidentiality, integrity, and availability of the Restricted Data? k. Have all applications undergone an application security test (a.k.a. web penetration test) by an independent security testing agency or team? If yes, please provide the detailed report for review. l. Do you perform static and/or dynamic source code review from a security perspective? If yes, please provide details. m. How does the application prevent users from downloading loan-level data? n. Does the application prevent users from re-identifying individuals from outliers or other methods in aggregated data? o. Does the service provide any of the following functionality to end users? - Email or messaging functionality (where a user can send emails or messages to arbitrary recipients. If only system generated emails are sent out, please reply 'No'). - Ability to browse external websites (from within the system/application). - Instant messaging or chat functionality. - File up or download by users? If yes, are these files scanned for malware? - Access from mobile devices? If yes, please specify if this access is through native apps on the device or using the mobile device browser.
Related body corporate	Where the loan level data may be made available to a representative that is a related body corporate of the applicant and the sponsor does not intend to enter into a separate data access deed with that related body corporate, the sponsor may wish to ask the applicant/user to confirm: a. that the policies, procedures and network security controls adopted by the related body corporate are substantially similar to the policies, procedures and controls applying to the applicant. b. that the related body corporate has not materially breached the *Privacy Act 1988* (Cth) or any similar privacy related laws. c. whether the related body corporate will be located in Australia or offshore.