DRAFT

Industry Aggregator Assurance Program

Review Scope and ASP Evaluation Criteria

This document sets out the Review Scope and ASP Evaluation Criteria. The Operating Committee will assess the ASP's proposal against the Evaluation Criteria to ensure ASP's proposal will deliver the Review at the minimum ~~expected~~ required standard of Reviews under the Program.

Principles of Review

- The Scope of this Review applies to all brokers within the Aggregator Group network i.e. ACL Holders and Credit Representatives.
- The Scope of this Review may be varied from time to time by resolution of the Operating Committee, including in response to legislative and regulatory changes as well as industry best practice.
- In completing Reviews, ASPs will prioritise evidence-based methodologies over self-assessment or attestation.
- The criteria set out in this document represents the minimum standard ~~expected~~ required for the Scope of Reviews conducted under the Program. The Operating Committee will consider innovative proposals from ASPs that would evaluate Aggregator Groups that go beyond the criteria set out in this document.
- Any deficiencies identified by a Review will be identified in the Report and recommendations will be provided to the relevant Aggregator for consideration.

Area of Focus 1: Onboarding & Accreditation of Brokers

Inherent Risk

Insufficient broker onboarding and ongoing due diligence processes completed by an Aggregator Group may result in a lender accreditation being provided to unsuitable individuals.

Risk Mitigation approach

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. a centralised onboarding & accreditation policy / framework in place that applies to all Australian Credit Licensee (ACL) and Credit Representative (CR) brokers;
ii. a set of competency and qualifications criteria for prospective brokers seeking accreditation (where relevant, these qualifications should be consistent with industry standards e.g. MFAA and FBAA);
iii. a due diligence review process for all new brokers seeking to join the Aggregator Group, which requires checking, at least, the following:
    - Broker identification;
    - Employment history and references, including, where relevant, references available under the ASIC reference checking protocol
    - Criminal history;
    - ASIC Banned & Disqualified Persons register;
    - Bankruptcy/Credit history;
    - Comprehensive negative media screening e.g. World Check; and
    - Sanctions and PEP Screening
iv. a due diligence review process (similar to the checks outlined in (iii) above) for existing brokers on an ongoing, periodic basis to confirm that the relevant broker continues to meet the Aggregator Group's policy requirements;
v. a due diligence review process (post onboarding and on an ongoing basis) to confirm that the broker's business, Directors and Responsible Managers maintain the required standards under ASIC Regulatory Guide 209 (Credit licensing: Responsible lending conduct);
vi. a process to manage exceptions (i.e. when a prospective or existing broker does not satisfy the Aggregator Group's criteria / due diligence requirements); and
a process to manage broker offboarding (e.g. transfers / exits).~~;~~
~~vi.~~ ~~a process to manage broker offboarding (e.g. transfers / exits),~~
vii.

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) reviewing the Aggregator Group's Onboarding & Accreditation policy / framework;
b) testing the effectiveness of the Aggregator Group's policy / framework by:
    - confirming whether relevant processes / procedures exist and are being performed in line with the relevant policy / framework;

- sampling a list of brokers to confirm whether they hold applicable industry memberships;
- sampling a list of newly accredited brokers and existing brokers (accredited > 12 months ago) to confirm that the relevant onboarding and ongoing due diligence processes are being adhered to;
- sampling a list of terminated brokers (adverse and non-adverse) to confirm that the relevant offboarding processes are being adhered to;
- sampling copies of references issued by the Aggregator Group, under ASIC's reference checking protocol, to confirm that the content is accurate and meaningful; and
- in all processes, confirm that exceptions to processes that are raised, are appropriately managed by the Aggregator Group;~~.~~

c) assessing the appropriateness of an Aggregator Group's record keeping practices, including but not limited to:
   - a register containing a list of all brokers' membership status;
   - a register containing a list of all brokers' credit license or credit representative status;
   - an exceptions management register; and
   - a register of all exited brokers and stored copies of any references provided under ASIC's reference checking protocol; and~~.~~

d) confirming that where required, communications to a lender was issued by the Aggregator Group in a timely manner (e.g. adverse terminations of brokers).

Area of Focus 2: Licensing & Membership Requirements

Inherent Risk:

Failure by an Aggregator Group to perform upfront and ongoing licensing checks and / or monitor compliance with licensing requirements may result in unlicensed individuals providing credit assistance.

Risk Mitigation Approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. a centralised register containing all applicable licence requirements for all brokers, including CRs and ACLs. The register should contain licence numbers and licence conditions;
ii. a process in place to identify structures / related parties of broker businesses operating under the Aggregator Group;
iii. a process in place to monitor changes made to structures / related parties of broker businesses, including for potential instances of shadow broking; ~~and~~
iv. a process in place to monitor and ensure that brokers are not providing financial product advice outside the licensing requirements (e.g. AFSL); and
v. processes in place to ensure accredited brokers compliance with licensing and industry body membership requirements, including but not limited to:
    - ASIC Breach Reporting requirements, consistent with ASIC Regulatory Guide 78;
    - internal dispute resolution mechanisms, consistent with ASIC Regulatory Guide 271;[1]
    - external dispute resolution mechanisms, consistent with ASIC Regulatory Guide 257;[2]
    - professional indemnity insurance policy~~;~~ consistent with ASIC Regulatory Guide 210;[3] and
    - minimum training and qualification requirements~~;~~ consistent with ASIC Regulatory Guide 206.[4]

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) obtaining evidence to confirm that the Aggregator Group maintains a register of all accredited brokers' (CRs and ACLs):
    - license numbers;
    - licence authorisations and conditions; and
    - certificate expiry and renewal dates.

[1] NCCPA, s 47(1)(h).
[2] NCCPA, s 47(1)(l).
[3] NCCPA, ss 47(1)(l), 48 (Requirements for compensation arrangements).
[4] NCCPA, s 47(1)(g); ASIC Regulatory Guide 206 (Credit licensing: Competence and Training).

b) sampling a list of brokers against the ASIC register to confirm that the Aggregator Group's centralised register is regularly maintained and updated, e.g. expired licenses / statuses are appropriately managed by the Aggregator Group;
c) sampling a list of brokers to confirm ongoing monitoring of brokers' compliance with all licensing and industry membership requirements is performed by the Aggregator Group. Where expiry or breaches of licensing requirements are identified, the ASP should also confirm that there is a process in place to notify lenders and brokers (and seek remediation);
d) sampling a list of all broker businesses operating under the Aggregator Group to confirm that the Aggregator Group takes reasonable steps to address any identified issues or changes with a broker business' structure / related parties / licensing structure; and
e) confirming that where required, communications to a lender was issued by the Aggregator Group in a timely manner (e.g. expired licenses or policy breaches relating to licensing requirements).

Area of Focus 3: Broker Governance and Professional Development

Inherent Risk:

Ineffective governance and oversight of broker practices, conduct and compliance with obligations, including ongoing professional development, may result in poor client outcomes.

Risk Mitigation Approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. ***in relation to the Aggregator Group's Risk Management*** – a centralised risk management policy and/or framework that details its risk appetite and strategy (e.g. risk assessment and action plan for risks that arise outside of the Aggregator's appetite);
ii. ***in relation to Broker Conduct Monitoring*** - a process in place to monitor broker conduct and broker's adherence to key obligations and legislative requirements. This process should include, but is not limited to, loan file reviews and assurance activities;
iii. ***in relation to Consequence Management*** - a defined consequence management policy / framework, that is applicable to all brokers accredited under the Aggregator Group;
iv. ***in relation to Complaints management*** - a defined complaints management policy / framework;
v. ***in relation to Referral Sources oversight*** - effective oversight over the eligibility and utilisation of referral sources within the Aggregator Group, including maintaining an appropriate referral source register;
vi. ***in relation to Broker Training & Development*** - a broker training and development policy / framework (for onboarding and on an ongoing basis) to ensure all accredited brokers remain at a high level of competency and fitness to provide credit assistance, consistent with ASIC Regulatory Guide 206 (Credit licensing: Competence and Training);
vii. the ability to track and monitor all accredited brokers' compliance with Continuing Professional Development (CPD) requirements; and
viii. a mentoring program to support new to industry and/or less experienced brokers.

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) reviewing the Aggregator Group's Risk Management policy / framework to confirm that the Aggregator Group has a defined risk appetite and assessment criteria;
b) obtaining evidence (e.g. quality assurance and compliance program) to confirm that the Aggregator Group performs ongoing monitoring of all brokers' conduct (ACLs and ACRs) and practices to ensure compliance with key obligations. This program should have:
    - a defined grading of broker risk e.g. a 'broker score';
    - a defined file sampling methodology, including standards that trigger an independent review; and

- a range of loan file reviews that covers in-progress and settled loans for all credit representatives and all credit license holders;

c) reviewing the effectiveness of the Aggregator Group's consequence management policy / framework. This should involve:
   - obtaining evidence to confirm that there is a process to identify, escalate and manage material broker issues, breaches and events and that process is operating effectively. This should also include evidence of notifying internal senior stakeholders, governance committees and lenders;
   - confirming that there is a process to ensure that relevant regulatory and industry bodies are appropriately notified of material breaches and/or events (i.e. to the same effect as section 912D of Corporations Act) and that process is operating effectively;
   - confirming that there is a process to inform and remediate clients who may have been impacted; and
   - assessing the appropriateness of an Aggregator Group's documentation of consequence management outcomes;
d) sighting the Aggregator Group's complaints register and confirming that:
   - complaints data are regularly and appropriately reviewed / analysed for trends;
   - complaints are appropriately escalated and managed by the Aggregator Group;
   - where required, lender/s have been notified of a complaint (e.g. complaint relating to a lender's Design & Distribution Obligations) in a timely manner; and
   - where required, the relevant broker has been notified of the complaint and an action plan devised by the Aggregator Group to resolve the complaint;
e) reviewing the operational effectiveness of the Aggregator Group's management of referral sources by confirming that the Aggregator Group has:
   - a defined eligibility criteria for referral sources;
   - a register containing a list of all known referral sources;
   - the ability to identify / monitor loans introduced via referral sources; and
   - evidence of consequence management actions taken against referral sources / brokers where processes have not been followed;
f) Reviewing the Aggregator Group's Training and Development policy / framework; and
g) testing the effectiveness of the Aggregator Group's Training and Development policy / framework by:
   - obtaining evidence to confirm that the Aggregator Group has the ability to track completion of mandatory ongoing training modules and CPD requirements for all brokers, credit representatives and credit license holders;
   - sighting the Aggregator Group's list of mandatory initial onboarding training modules and ongoing training modules to ensure that there is adequate coverage of key legislative requirements (e.g. AML / CTF, Privacy, Responsible Lending);
   - sampling cases of compliance and non-compliance with all training requirements (including CPD) and reviewing the effectiveness of the Aggregator Group's consequence management actions;
   - sampling examples of where the Aggregator Group has followed the process in place to provide training support to brokers that have not submitted a loan for an period greater than 6 months; and
   - confirming the Aggregator Group has an adequate mentoring program in place to support new to industry brokers (this should include clear requirements for mentoring

relationships). Including sampling of mentor training plans for new to industry brokers and assessment of suitability.

Area of Focus 4: Management of Regulations

Responsible Lending

Inherent Risk:

Insufficient frameworks and/or monitoring of broker's compliance with Responsible Lending obligations by an Aggregator Group may result in a breach of legislative requirements and poor customer outcomes.

Risk Mitigation approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. a centralised Responsible Lending policy / framework that applies to all ACL and CR brokers;
ii. clear guidance, training, and processes for all brokers to comprehensively understand their Responsible Lending obligations, including but not limited to brokers:
    - making reasonable inquiries into the customer's financial situation and requirements & objectives;
    - taking reasonable steps to verify the customer's financial situation; [5]
    - making a preliminary assessment of the mortgage loan application based on the customer's financial situation and requirements and objectives; [6]
    - assessing whether a mortgage loan is 'not unsuitable' for a customer applying the statutory presumptions; [7]
    - keeping a record of materials that form the basis of the preliminary assessment; [8] and
    - refraining from suggesting that customers should enter or remain in unsuitable credit contracts;. [9]
iii. appropriate controls and guidance for all brokers to ensure the issue, collection and storing of key documents that support compliance with Responsible Lending obligations (e.g. Broker interview guide, Preliminary Assessment Form etc.) is adhered to;
iv. appropriate controls to manage in-flight changes to a loan contract and variations to existing loan contracts;
v. appropriate controls to ensure that all brokers are complying with AML and CTF / KYC obligations and appropriately disclosing their "method of interview" and "method of identification"; and
vi. a quality assurance/loan file review process to ensure all brokers are complying with their Responsible Lending obligations. Sampling should include loan files for all brokers, credit

[5] *National Consumer Credit Protection Act 2009* (Cth) (**NCCPA**), ss 117 (reasonable inquiries and reasonable steps to verify).

[6] NCCPA, s 116 (preliminary assessment of unsuitability).

[7] NCCPA, ss 118 (criteria for assessing unsuitability – entering contract or increasing the credit), 119 (When the credit contract must be assessed as unsuitable—remaining in credit contract).

[8] To ensure the broker is capable of complying with any requests made by an applicant for a copy of a preliminary assessment under NCCPA, s 120.

[9] NCCPA, ss 123 (suggesting or assisting consumers to enter, or increase the credit limit under, unsuitable credit contracts), 124 (suggesting to consumers to remain in unsuitable credit contracts).

representatives and credit licence holders and be linked to the Aggregator Group's grading of broker risk e.g. 'broker score'.

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) sighting the Responsible Lending policy / framework and confirming that this policy / process is operating in line with the relevant Responsible Lending legislation and regulatory requirements;
b) confirming that the Aggregator Group actively reviews and implements changes in legislation where it relates to Responsible Lending;
c) sampling loan application files that have been reviewed by the Aggregator Group's loan file review program during a test period to check the following:
    - sufficient inquiries and verification steps have been completed by the broker;
    - preliminary assessments of the customer's financial situation, requirements & objectives have been completed;
    - required supporting documentation and information (e.g. broker interview guide, preliminary assessment form, income verification documentation, broker notes) have been retained in loan file records;
    - in-flight changes made to a loan application or contract variation request should be documented and assessed against responsible lending requirements;
    - where required, communication of key findings and/or feedback to brokers have been completed by the Aggregator Group; and
    - where non-compliance is identified, appropriate consequence management has been issued to the broker and this is reflected in an updated grading of broker risk e.g. 'broker score'; and.
d) confirming that the Aggregator Group has a process in place to comply with AML and CTF / KYC requirements including maintaining oversight of brokers' "method of interview" and "method of identification".

Best Interest Duty (BID)

Inherent Risk:

Insufficient training, system and ongoing monitoring of controls in place to ensure broker's compliance with Best Interest Duty obligations may result in a breach of legislative requirements and poor customer outcomes.

Risk Mitigation approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. clear guidance, training, and processes for all brokers to comprehensively understand their BID obligations, including to act in the best interests of the clients[10] and prioritising the clients' interest in the event of a conflict of interest (including to the extent that there is a conflict of interest between an applicant and a mortgage broker e.g. due to commission)[11] ;
ii. a process to manage system changes to key broker interfaces, including CRM, to uphold compliance with BID; and
iii. a process to monitor broker conduct to ensure compliance with BID and where required, perform remediation activity.

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) reviewing the Aggregator Group's BID policies and/or processes (if any) and confirming that this policy / process is operating in line with the relevant BID legislation and regulatory requirements;
b) sighting the Aggregator Group's training modules and sample communications delivered to brokers to reinforce BID obligations;
~~b)~~c) reviewing system controls (i.e. within CRM) and compliance controls that assist the Aggregator Group in maintaining oversight over brokers' adherence to BID requirements. This may involve reviewing audit checklists and loan file review reports to identify if previous findings of non-compliance with BID were appropriately remedied;
~~c)~~d) reviewing the Aggregator Group's Conflict of Interest policy / framework; and
~~d)~~e) obtaining evidence to confirm that the Aggregator Group appropriately records, monitors and manages conflicts of interest and instances of conflicted remuneration/soft dollar benefits. This should include sampling of individual conflicts to assess how they are being managed on an ongoing basis. Where non-compliance is observed, assess whether appropriate consequence management has been applied.

Conflicts of Interest

Inherent Risk

Insufficient training and oversight in place to ensure that Conflicts of Interests are appropriately identified, reported and managed may result in a breach of legislative requirements and poor customer outcomes.

Risk Mitigation approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. a Conflict of Interest policy / framework covering the identification, reporting and management of potential conflicts of interest;

[10] NCCPA, ss 158LA (Licensee must act in the best interests of the consumer), s 158LE (Credit representative must act in the best interests of the consumer).

[11] NCCPA, ss 158LB (Conflict between consumer's interests and those of the licensee etc), 158LF (Conflict between consumer's interests and those of the credit representative etc).

ii. a policy that governs the giving and receiving of potentially conflicted remuneration, including soft dollar benefits and an associated register to record actual and/or potential instances; and
iii. a register to record conflicts of interest and/or potential conflicts of interest, which is reviewed and updated regularly.

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) reviewing the Aggregator Group's Conflict of Interest policy / framework; and
b) obtaining evidence to confirm that the Aggregator Group appropriately records, monitors and manages conflicts of interest and instances of conflicted remuneration/soft dollar benefits. This should include sampling of individual conflicts to assess how they are being managed on an ongoing basis. Where non-compliance is observed, assess whether appropriate consequence management has been applied.

DDO

Inherent Risk:

Insufficient support provided or oversight of mortgage brokers' compliance with DDO by an Aggregator Group may result in a breach of legislative requirements and poor customer outcomes.

Risk Mitigation approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. clear guidance, training, and processes for all brokers to comprehensively understand their obligations under DDO regulations;
ii. adequate controls or 'reasonable steps' to ensure that brokers:
    - do not distribute a product without a Target Market Determination (TMD); [12]
    - are selling the lender's products within the relevant lender's TMD;[13] and
    - utilise marketing and promotional materials that are consistent with the relevant TMDs;
iii. a process in place to ensure that complaints relating to a lender's products are appropriately recorded and escalated to the relevant lender within the prescribed timeframes; and
iv. a process in place to identify significant dealings and notify the relevant lender of any such occurrence. [14]

Evaluation Criteria:

[12] *Corporations Act* 2001 (Cth) (**Corporations Act**), s 994D.
[13] Corporations Act, s 994E(3).
[14] Corporations Act, s 994G.

At a minimum, an Assurance Service Provider should assess this by :

a) sampling communications of lenders' TMDs issued by the Aggregator Group to all brokers to confirm adequacy and timeliness in communication;
b) evidence of TMDs being made available/accessible to brokers;
c) sighting the Aggregator Group's controls or 'reasonable steps' taken to comply with DDO requirements;
d) sighting the Aggregator Group's process for identifying and recording complaints relating to a lender's product. If available, evidence should be obtained to demonstrate that escalation of these complaints to the relevant lender occurred within the prescribed timeframes; and
e) sighting the Aggregator Group's process for identifying and recording significant dealings relating to a lender's product. If available, evidence should be obtained to demonstrate that notification of significant dealings to the relevant lender occurs within the prescribed timeframes.

Breach Reporting

Inherent Risk:

If an Aggregator Group has inadequate frameworks or processes in place to manage compliance with the applicable Breach Reporting legislation, this may result in regulatory and reputational impact to the lender.

Risk Mitigation approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. a process in place to identify and report significant breaches to a regulator (irrespective of whether the breaches are committed by the Aggregator Group, individual broker or brokers under an independent ACL); and
ii. a process in place to notify the relevant lender of any reportable breaches that relate to that lender.

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) reviewing the Aggregator Group's process for identifying and reporting significant breaches to a regulator;
b) sampling reportable breach notifications reported by the Aggregator Group to assess for compliance with the relevant ASIC Breach Reporting requirements; and
c) reviewing evidence to demonstrate that the Aggregator Group has a process to notify Lenders impacted by any reportable breaches.

Reference Checking

Inherent Risk:

If an Aggregator Group is not compliant with their obligations under the applicable legislative framework for reference checking, this may result in regulatory and reputational impact to the Lender.

Risk Mitigation approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have a process in place to perform reference checking (and provide references upon request) on individuals seeking to be employed or authorised as a broker in the Aggregator Group.[15]

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by obtaining evidence of appropriate reference checking being completed (including samples of references provided) by the Aggregator Group.

[15] NCCPA, s 47(1)(EA).

Area of Focus 5: IT and System Access Controls

Inherent Risk

If an Aggregator Group does not maintain adequate frameworks and appropriately identify, monitor and test key IT systems, unauthorised or unintended access to customer data may occur.

Risk Mitigation approach

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. an IT Policy / Framework in place covering its key systems and platforms;
ii. current and accurate mapping of information flows between an Aggregator Group's loan application platform to the relevant Lender gateway (e.g. ApplyOnline and Simpology);
iii. appropriate user access system validation controls, which are performed and tested on a periodic basis to prevent inappropriate access to the Aggregator Group's systems;
iv. an IT Change Management Policy / Framework in place to guard against inappropriate deployment of:
    - changes to applications / software (e.g. back – up processes, password policy, retention of hard copy files, cloud services availability); and
    - modifications to data (e.g. clear processes and controls around data migration activities); and
v. clear processes and controls around data migration / modification activities (e.g. performance of testing and reconciliation).

Evaluation Criteria

At a minimum, an Assurance Service Provider should assess this by:

a) reviewing the Aggregator Group's IT Policy / Framework and IT Change Management Policy / Framework;
b) testing the effectiveness of the Aggregator Group's Policy / Framework by:
    - confirming whether relevant processes / procedures exist and are being performed in line with the relevant Policy / Framework;
    - obtaining evidence to confirm that information flows are being monitored for accuracy and where required, remediated effectively;
    - obtaining evidence (e.g. internal reports or sampling) to confirm that user access validation testing is periodically performed, reviewed and where required, that steps are taken to remove superseded access requirements;
    - obtaining evidence to confirm that the Aggregator Group performs data migration testing, prior to commencing migration / modification, (e.g. to ensure loan application data is transferred completely and accurately); and
    - obtaining evidence to confirm that appropriate steps are taken to remedy any identified defects in any IT and System Access controls.

Area of Focus 6: Privacy and Customer Data Security

Inherent Risk

If an Aggregator Group (and their associated mortgage brokers) do not appropriately secure customer information, in compliance with applicable privacy laws and regulations, this may result in regulatory and reputational impact to the lender, as well as poor customer outcomes.

Risk Mitigation approach

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. a Privacy policy / framework, which outlines key requirements under the Australian Privacy legislation and regulations (including Office of the Australian Information Commissioner reporting obligations and process for identifying, escalating and managing notifiable data breaches);
ii. appropriate training provided to its staff and brokers to ensure compliance with Australian Privacy legislation and regulations;
iii. protocols in place to ensure that customer and broker information collected / retained is only used for the purpose for which it was collected / retained, in accordance with the applicable Privacy legislation and regulations;
iv. adequate controls in place to monitor the transfer of customer data from the Aggregator Group's key systems to external parties and / or between brokers;
v. a clear understanding of how and where their customer data is sourced / stored (e.g. if customer data is stored in a particular jurisdiction, that privacy implications of that jurisdiction are identified and appropriately managed);
vi. a process in place to manage changes made to a "broker of record", including but not limited to, notifications to the relevant lender and the re-obtaining of customer consent (where required), prior to the new broker having access to customer information;
vii. appropriate security measures (e.g. firewalls and anti-virus software) that are regularly tested to address the threat of malicious electronic attacks;
viii. appropriate management of physical IT equipment (e.g. hardware);
ix. an appropriate Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP); and
x. a process in place to ensure regular testing and back-up of data and critical systems is performed.

Evaluation Criteria

At a minimum, an Assurance Service Provider should assess this by:

a) reviewing the Aggregator Group's Privacy policy / framework and confirming that this policy / framework is operating in line with the relevant Australian Privacy legislation and regulatory requirements;
b) testing the effectiveness of the Aggregator Group's policy / framework by:
    - sighting the Aggregator Group's privacy training and data breach requirement modules to assess the effectiveness of these training programs (i.e. that Aggregator Group's staff and brokers have a clear understanding of key privacy requirements and that where required, appropriate remedial action (e.g. re-training) is assigned);

- sighting protocols and processes relating to data collection, transfer, destruction and retention arrangements (applicable to Aggregator Group's staff and brokers);
- sampling a list of "broker of record" changes in the test period to confirm that this process is managed appropriately;
- obtaining evidence to confirm that appropriate and adequate security testing (for software / cloud and physical IT environments) is being performed and that findings are remediated; and
- sighting the Aggregator Group's BCP and DRP and obtaining evidence to confirm that appropriate and regular testing is performed; and.

c) confirming that where required, communications to a Lender was issued by the Aggregator Group in a timely manner (e.g. notifiable data breach notifications, broker of record changes).

Area of Focus 7: Outsourced / Offshore Third-Party Management

Inherent Risk:

If an Aggregator Group does not have adequate upfront and/or ongoing governance and oversight on outsourced or offshore functions, third party organisations could be onboarded or maintained in a manner that is inconsistent with industry standards or contractual agreements.

Risk Mitigation approach:

To mitigate this Risk, a lender would expect an Aggregator Group to have:

i. an outsourcing/ offshoring policy that covers appropriate due diligence, including, for example, Privacy, AML/CTF and World Checks;
ii. appropriate contractual agreements in place to document third-party arrangements and obligations;
iii. a process in place to identify and assess risks associated with third party organisations, in line with the Aggregator Group's risk appetite; and
iv. a process in place to regularly monitor the performance of offshored and/or outsourced functions, to ensure compliance with obligations stipulated in contractual agreements and Service Level Agreements (SLA).

Evaluation Criteria:

At a minimum, an Assurance Service Provider should assess this by:

a) sighting the Aggregator Group's outsourcing/offshoring policies;
b) sampling outsourcing/offshoring third party contractual arrangements, to ensure that appropriate due diligence has been performed and approved by senior management; and
c) obtaining evidence of monitoring being performed by the Aggregator Group to ensure adherence to obligations stipulated in contractual agreements and SLAs.