FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

FDIC Commercial Real Estate Due Diligence

RSM US, LLP

(RECVR-14-G-0536)

Date Approved by Chief Privacy Officer (CPO)/Designee: 03/31/2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The FDIC maintains stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions (FIs), and managing receiverships. The FDIC Division of Resolutions and Receiverships (DRR) is responsible for resolving failed or failing FDIC-insured depository FIs, which include among other important responsibilities, effectively and efficiently managing and disposing assets held by the FIs. FDIC DRR has contracted the due diligence services of RSM US LLP (RSM) to support the overall disposition of commercial real estate assigned assets from failed FDIC-insured depository FIs which include financial analysis, due diligence reviews, and valuation of commercial real estate assigned assets.

The scope of work under due diligence services includes: data capture aggregation and analysis; documentation file review; underwriting review; regulatory compliance review; ordering broker price opinions (BPOs); credit quality and servicing operation assessment; and imaging, indexing and uploading loan documentation to a secure, web-based data repository for a group of loans to be identified (hereinafter referred to as the "loan population"). The required services include verifying real property values and valuation services. Once the due diligence services begin, RSM shall coordinate and work cooperatively as necessary with the FDIC marketing/sale specialists and other contacts, the lead underwriter, the interim and/or securitization servicers, FDIC legal counsel, FDIC accountants and any other interested party identified by the FDIC throughout the performance under each Task Order.

SECTION II – DATA TYPE, SOURCES, AND USE

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

Data Collected from Financial Institution

Onsite at the FI, RSM receives hard copy loan documents to be scanned (imaged) to an encrypted contractor-provided laptop using an FDIC-provided scanner. Loan documents provided to RSM for imaging and indexing may include PII about the guarantors[1] of the commercial loans. This PII may include the guarantor's full name, date of birth, social security number (SSN), employment status, home address, personal phone number, personal email address, financial information, legal documents, and military status. The data is later uploaded to the FDIC Virtual Data Room (VDR)[2] as described in Q7a, where it will be subject to contractor-conducted due diligence reviews.

[1] A guarantor loan is a type of unsecured loan that requires a guarantor to co-sign the credit agreement. A guarantor is a person who agrees to repay the commercial loan's debt should the entity responsible defaults on agreed repayments.

[2] The FDIC's VDR is a secure website facility and technology provided by a private sector service provider. The VDR service is used by DRR to create workspaces for failing or failed FI projects, where confidential documents and information can be rapidly exchanged with specific groups of authorized internal and external users. For example, DRR staff use the VDR to provide extensive information to bidders about the failing FI and the marketing process. Loan and deposit database files, general ledgers and other performance reports, as well as detailed operations information, are provided on the secured website. DRR staff may also provide imaged loan files for larger failing FIs if time permits. The VDR is also used to share information with regulators on bidder activity to ensure that interested bidders are eligible to bid. For additional information, refer to the FDIC's VDR Privacy Impact Assessment at www.fdic.gov.

Data Collected from FDIC Staff

FDIC DRR's Post Closing Asset Manager (PCAM)[3] may upload imaged loan documents to the FDIC VDR for due diligence reviews by RSM. The imaged loan documents may include PII such as the guarantor's full name, date of birth, SSN, employment status, home address, personal phone number, personal email address, financial information, legal documents, and military status. After review of the loan documents, RSM personnel completes and uploads a structured loan-by-loan analysis and detailed final report of the loan population onto the FDIC VDR for DRR to use while managing assets. The loan-by-loan analysis may include a limited subset of the PII referenced above; the final report does not contain any PII. All compliance assurance work is completed internally at RSM for the assigned assets.

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

The data is collected and maintained to support and facilitate DRR's disposition of assets that are obtained from failed FDIC-insured depository FIs. Accordingly, the data may be used in the conduct of due diligence reviews, including file reviews, underwriting reviews, regulatory compliance reviews, and other related resolution activities.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above? *(This is not intended to be an all-inclusive list. Specify other categories of PII, as needed.*):

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☐	☒
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s) (non-work)	☒	☐
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☐	☒
Criminal Information	☐	☒
Military Status and/or Records	☒	☐
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: Mortgage Documents)	☒	☐

[3] The PCAM is the FDIC on-site Asset Manager tasked with marketing and selling assets owned by the Receivership.

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs:

As part of the services for the due diligence work, RSM is responsible for imaging and indexing loan documents from the failed FI and uploading them to the FDIC VDR. The loan documents collected, imaged and indexed may contain SSNs. Also, imaged loan documents provided by the FDIC Post Closing Group via the FDIC VDR to RSM may contain SSNs as well. The collection of SSNs is incidental to the collection, imaging and indexing of loan documents, and is not required for the scope of work being conducted. SSNs are not utilized for the final deliverables provided back to the FDIC.

b) Provide the legal authority which permits the collection of SSNs.

The collection of SSNs is incidental to the collection, imaging and indexing of loan documents, and is not required for the scope of work being conducted.
Sections 9, 11, and 13 of the Federal Deposit Insurance Act (12 U.S.C. 1819, 1821, and 1823) and applicable State laws provide the legal authority governing the liquidation of assets and wind-up of the affairs of failed financial institutions.

c) Identify whether the SSN is masked or otherwise truncated within the system:

The SSNs contained on documents imaged by RSM and uploaded to the FDIC VDR by RSM may or may not be masked or truncated. As noted earlier, the collection and maintenance of any SSNs is incidental to the collection, imaging and indexing of loan documents by RSM.

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☒	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☐
5,001 – 7,500 ☐	7,501 – 10,000 ☐	10,001 – 50,000 ☐	50,001 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[4]:

To date, RSM has not been awarded any task orders under this agreement. In the event of a major crisis, the number of estimated records that contain PII may be as high as 100,000 depending upon the failed FI.

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[5] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
7a. Collected from Failed	Authorized RSM personnel collect asset-level loan document data,	☒ Yes ☐ No

[4] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

[5] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

Financial Institutions (FIs) During Onsite Reviews	which may contain some or all of the PII specified in Q4, during their onsite reviews at the failed FI. RSM receives hard copy loan documents at the FI, which they scan (image) to an encrypted contractor-provided laptop using an FDIC-provided scanner. Authorized RSM staff transport (i.e., hand-carry) the encrypted laptop from the FI site to their Chicago, IL office where they transfer the data from that encrypted laptop to other encrypted laptops assigned to RSM staff, where the imaged loan files are indexed and uploaded to the FDIC VDR. Once the documents have been uploaded to the FDIC VDR, each RSM laptop is wiped clean to ensure that no PII/SI remains on the laptop. All RSM laptops are full disk encrypted. Once the work for the project is completed, the encrypted laptop that was initially used to collect the scanned images at the FI is wiped clean of all imaged loan documents.	
7b. Collected from FDIC Staff	Authorized FDIC DRR Post Closing staff upload imaged loan documents, which may include the PII specified in Q4, into RSM's respective folder on the FDIC VDR. After review of the loan documents, RSM personnel complete and upload a structured loan-by-loan analysis and detailed final report of the loan population onto the FDIC VDR for DRR use. In drafting the final due diligence report for the FDIC, RSM may work with the FDIC Oversight Manager (OM) on the review and approval of the final due diligence report via the FDIC Secure Email Service. There is no PII included on the final due diligence report.	☒ Yes ☐ No

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

Yes, data may be retrieved by personal identifiers such as the loan number, guarantor's name, address, or SSN.

9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

30-64-0013, *Insured Financial Institution Liquidation Records.*

This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
  - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 through 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that will access or receive PII data as part of the outsourced service/project. ***(Check "No" or "Yes" for each category. For each category checked "Yes," specify who will have access to, be provided with, or maintain the PII, what PII elements will be accessed/shared/maintained by them, how the access or sharing will occur, and the purpose and use of this PII.)***

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	Authorized RSM personnel performing the work on behalf of the FDIC have access to asset loan document data, which may contain PII as specified in Question 4, in order to conduct due diligence efforts, provide valuation assessments and advice regarding commercial real estate FI loans. Specifically, RSM personnel who may have access to PII include: RSM's Project Manager for purposes of overseeing onsite reviews, due diligence, and portfolio valuations/assessments; Senior Underwriters and other Underwriters for purposes of making valuation decisions and helping prepare reports; Financial Analysts for report analysis and preparation; and Administrative Staff who are in charge of uploading the data to the FDIC VDR.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	RSM shares their final due diligence reports and the indexed loan files with the FDIC via the FDIC VDR. There is no PII included on the final due diligence report. The indexed loan data files may include any of the PII specified in Question 4. In drafting the final due diligence report for the FDIC, RSM may work with the FDIC OM on the review and approval of the final due diligence report via the FDIC Secure Email Service. Authorized FDIC/DRR personnel post the final due diligence reports in a secure FDIC/DRR SharePoint site. These reports are utilized by FDIC/DRR for the purposes detailed in Question 3, such as to resolve loan assets in a manner that is most cost-effective or determine the consideration offered to the FI by the FDIC, as applicable.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	Not Applicable.
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☐	☒	Not Applicable.
10e. Federal, State, and/or Local Agencies	☐	☒	Not Applicable.
10f. Other	☐	☒	Not Applicable.

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	☒	☐
FDIC Confidentiality Agreement (Individual)	☒	☐
Non-Disclosure Agreement (NDA)	☒	☐
Memoranda of Understanding (MOU)	☐	☒
Information Sharing Agreements (ISA)	☐	☒
Authentication Risk Assessment	☐	☒
Other Applicable Agreement(s) (*Specify*: _____)	☐	☒

If you answered NO to any item above, please provide additional information if available:

RSM is an outsourced service provider and therefore is not subject to MOUs or ISAs.

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☐ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information.

☐ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information. ***(Explain how individuals may decline or consent to the use of their information.):***

☒ Not applicable. Information is not collected directly from individuals.

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No

☐ Yes *(If yes, check applicable box(es) below.)*

- ☐ Link to FDIC Privacy Policy
- ☐ FDIC Privacy Act Statement
- ☐ Contractor Privacy Policy or Statement
- ☐ No Privacy Policy has been posted

☒ Not applicable

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care. ***[Provide the name of the Outsourced Service Provider and check all applicable box(es).]***

☒ RSM has gone through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☒ YES

☒ The FDIC conducts background investigations (BIs) on key RSM personnel and other applicable personnel prior to their beginning work on the contract.

☒ RSM is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsource Service Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements.

☐ Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) ***Attach the Contract Clause Verification Checklist to the back of this form.***

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date? ***[Check all applicable box(es) and insert the appropriate response and System/Project name.]***

☒ Data is collected directly from the failed financial institutions. As such, the FDIC and its vendors rely on the financial institutions to provide accurate data.

☒ The vendor/contractor works with FDIC to verify the integrity of the data before inputting it into the system or using it to support the project.

☒ As necessary, RSM's Project Manager checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☐ Other (*Please explain*.)

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider. (*Check all applicable box(es) and insert the name of the Outsourced Information Service Provider and title of the firm's senior management official.*)

☒ Within FDIC, RSM's Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy

Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

☒ Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated Project Manager to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

☒ The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

During on-site reviews, RSM receives hard copy loan documents to be scanned (imaged) to an encrypted contractor-provided laptop using an FDIC-provided scanner. The encrypted laptop is utilized for temporary storage of data until RSM transfers the data from the encrypted laptop to other encrypted laptops assigned to RSM staff, where the imaged loan files are indexed and uploaded to the FDIC VDR.

Once the documents have been uploaded to the FDIC VDR, each RSM laptop is wiped clean to ensure that no PII/SI remains on the laptop. Once the project is completed, the encrypted laptop that was initially used to collect the scanned images at the FI is wiped clean of all imaged loan documents.

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

As specified in the contact between FDIC and RSM, once the data is uploaded to the VDR, the encrypted laptops used for the imaging work are cleared of the imaged loan documents by RSM. RSM has their file servers purged of sensitive data three years after completion of the due diligence work. The contractor must dispose or return the data "as FDIC directs" "Upon completion or termination of the contract, or at any time the Contracting Officer requests it in writing" per contract clause 7.4.2-2(b).