FORM NRSRO

OMB APPROVAL
OMB Number: 3235-0625
Expires: Dec. 31, 2026
Estimated average burden hours per response: 36

APPLICATION FOR REGISTRATION AS A NATIONALLY RECOGNIZED STATISTICAL RATING ORGANIZATION (NRSRO)

SEC 1541 (1-24)

Persons who respond to the collection of information contained in this form are not required to respond unless the form displays a currently valid OMB control number.

APPLICATION FOR REGISTRATION AS A NATIONALLY RECOGNIZED STATISTICAL RATING ORGANIZATION (NRSRO)

☐ INITIAL APPLICATION

☐ APPLICATION TO ADD CLASS OF CREDIT RATINGS

☐ APPLICATION SUPPLEMENT
Items and/or Exhibits Supplemented:

_____

☐ ANNUAL CERTIFICATION

☑ UPDATE OF REGISTRATION
Items and/or Exhibits Amended:
Item 3 Exhibits 2,3 and 4

☐ WITHDRAWAL FROM REGISTRATION

Important: Refer to Form NRSRO Instructions for General Instructions, Item-by-Item Instructions, an Explanation of Terms, and the Disclosure Reporting Page (NRSRO). "You" and "your" mean the person filing or furnishing, as applicable, this Form NRSRO. "Applicant" and "NRSRO" mean the person filing or furnishing, as applicable, this Form NRSRO and any credit rating affiliate identified in Item 3.

1. **A.** Your full name:

Clasificadora de Riesgo Pacific Credit Rating S.A.C.

B. **(i)** Name under which your credit rating business is primarily conducted, if different from Item 1A:

PCR

(ii) Any other name under which your credit rating business is conducted and where it is used (other than the name of a credit rating affiliate identified in Item 3):

N/A

C. Address of your principal office (do not use a P.O. Box):

Av. El Derby No.254,	Lima	Peru	15023
(Number and Street)	(City)	(State/Country)	(Zip/Postal Code)

D. Mailing address, if different:

(Number and Street)	(City)	(State/Country)	(Zip/Postal Code)

E. Contact person (See Instructions):

Oscar Jasaui	President
(Name and Title)	

Av. El Derby No. 254,	Lima	Peru	15023
(Number and Street)	(City)	(State/Country)	(Zip/Postal Code)

CERTIFICATION:

The undersigned has executed this Form NRSRO on behalf of, and on the authority of, the Applicant/NRSRO. The undersigned, on behalf of the Applicant/NRSRO, represents that the information and statements contained in this Form, including Exhibits and attachments, all of which are part of this Form, are accurate in all significant respects. If

this is an ANNUAL CERTIFICATION, the undersigned, on behalf of the NRSRO, represents that the NRSRO's application on Form NRSRO, as amended, is accurate in all significant respects.

5/4/2026 (Date) Clasificadora de Riesgo Pacific Credit Rating S.A.C. (Name of the Applicant/NRSRO)

By: /S/ Oscar Jasaui (Signature) Oscar Jasaui, President (Print Name and Title)

2. **A**. Your legal status:

☑ Corporation ☐ Limited Liability Company ☐ Partnership ☐ Other (specify) _____

B. Month and day of your fiscal year end: 12/31

C. Place and date of your formation (i.e., state or country where you were incorporated, where your partnership agreement was filed, or where you otherwise were formed):

State/Country of formation: Lima, Peru Date of formation: 2/1/95

3. Your credit rating affiliates (See Instructions):

Item 3 is attached and made a part of this form NRSRO

(Name) (Address)

(Name) (Address)

(Name) (Address)

(Name) (Address)

(Name) (Address)

4. The designated compliance officer of the Applicant/NRSRO (See Instructions):

Rafael Colado Ibarreche Designated Compliance Officer
(Name and Title)

Corporativo Coyoacan Mexico Mexico 03100
(Number and Street) (City) (State/Country) (Postal Code)

5. Describe in detail how this Form NRSRO and Exhibits 1 through 9 to this Form NRSRO will be made publicly and freely available on an easily accessible portion of the corporate Internet website of the Applicant/NRSRO (See Instructions):

Form NRSRO and Exhibits 1 through 9 will be publicy available free of charge of our website www.ratingspcr.com

6. COMPLETE ITEM 6 ONLY IF THIS IS AN INITIAL APPLICATION, APPLICATION SUPPLEMENT, OR APPLICATION TO ADD A CLASS OF CREDIT RATINGS.

A. Indicate below the classes of credit ratings for which the Applicant/NRSRO is applying to be registered. For each class, indicate the approximate number of obligors, securities, and money market instruments in that class as of the date of this application for which the Applicant/NRSRO has an outstanding credit rating and the approximate date the Applicant/NRSRO began issuing credit ratings as a "credit rating agency" in that class on a continuous basis through the present (See Instructions):

Class of credit ratings	Applying for registration	Approximate number currently outstanding	Approximate date issuance commenced
financial institutions as that term is defined in section 3(a)(46) of the Exchange Act (15 U.S.C. 78c(a)(46)), brokers as that term is defined in section 3(a)(4) of the Exchange Act (15 U.S.C. 78c(a)(4)), and dealers as that term is defined in section 3(a)(5) of the Exchange Act (15 U.S.C. 78c(a)(5))	☐		
insurance companies as that term is defined in section 3(a)(19) of the Exchange Act (15 U.S.C. 78c(a)(19))	☐		
corporate issuers	☐		
issuers of asset-backed securities as that term is defined in 17 CFR 229.1101(c)	☐		
issuers of government securities as that term is defined in section 3(a)(42) of the Exchange Act (15 U.S.C. 78c(a)(42)), municipal securities as that term is defined in section 3(a)(29) of the Exchange Act (15 U.S.C. 78c(a)(29)), and foreign government securities	☐		

B. Briefly describe how the Applicant/NRSRO makes the credit ratings in the classes indicated in Item 6A readily accessible for free or for a reasonable fee (See Instructions):

_____

_____

_____

C. Check the applicable box and attach certifications from qualified institutional buyers, if required (See Instructions):

☐ The Applicant/NRSRO is attaching _____certifications from qualified institutional buyers to this application. Each is marked "Certification from Qualified Institutional Buyer."

☐ The Applicant/NRSRO is exempt from the requirement to file certifications from qualified institutional buyers pursuant to section 15E(a)(1)(D) of the Exchange Act.

Note: You are not required to make a Certification from a Qualified Institutional Buyer filed with this Form NRSRO publicly available on your corporate Internet website pursuant to Exchange Act Rule 17g-1(i). You may request that the Commission keep these certifications confidential by marking each page "Confidential Treatment" and complying with Commission rules governing confidential treatment. The Commission will keep the certifications confidential upon request to the extent permitted by law.

7. DO NOT COMPLETE ITEM 7 IF THIS IS AN INITIAL APPLICATION.

A. Indicate below the classes of credit ratings for which the NRSRO is currently registered. For each class, indicate the approximate number of obligors, securities, and money market instruments in that class for which the NRSRO had an outstanding credit rating as of the most recent calendar year end and the approximate date the NRSRO began issuing credit ratings as a "credit rating agency" in that class on a continuous basis through the present (See Instructions):

Class of credit rating	Currently registered	Approximate number outstanding as of the most recent calendar year end	Approximate date issuance commenced
financial institutions as that term is defined in section 3(a)(46) of the Exchange Act (15 U.S.C. 78c(a)(46)), brokers as that term is defined in section 3(a)(4) of the Exchange Act (15 U.S.C. 78c(a)(4)), and dealers as that term is defined in section 3(a)(5) of the Exchange Act (15 U.S.C. 78c(a)(5))	☑	490	1995
insurance companies as that term is defined in section 3(a)(19) of the Exchange Act (15 U.S.C. 78c(a)(19))	☐		
corporate issuers	☑	573	1995
issuers of asset-backed securities as that term is defined in 17 CFR 229.1101(c)	☐		
issuers of government securities as that term is defined in section 3(a)(42) of the Act (15 U.S.C. 78c(a)(42)), municipal securities as that term is defined in section 3(a)(29) of the Exchange Act (15 U.S.C. 78c(a)(29)), and foreign government securities	☑	36	1995

B. Briefly describe how the NRSRO makes the credit ratings in the classes indicated in Item 7A readily accessible for free or for a reasonable fee (See Instructions):

Credit ratings in Item 7A are available by press release and electronic notification and are accesible free of charge at PCR´s website www.ratingspcr.com

8. Answer each question. Provide information that relates to a "Yes" answer on a Disclosure Reporting Page (NRSRO) and submit the Disclosure Reporting Page with this Form NRSRO (See Instructions). You are not required to make any disclosure reporting pages submitted with this Form publicly available on your corporate Internet website pursuant to Exchange Act Rule 17g-1(i). You may request that the Commission keep any disclosure reporting pages confidential by marking each page "Confidential Treatment" and complying with Commission rules governing confidential treatment. The Commission will keep the disclosure reporting pages confidential upon request to the extent permitted by law.	

	YES	NO
A. Has the Applicant/NRSRO or any person within the Applicant/NRSRO committed or omitted any act, or been subject to an order or finding, enumerated in subparagraphs (A), (D), (E), (G), or (H) of section 15(b)(4) of the Securities Exchange Act of 1934, been convicted of any offense specified in section 15(b)(4)(B) of the Securities Exchange Act of 1934, or been enjoined from any action, conduct, or practice specified in section 15(b)(4)(C) of the Securities Exchange Act of 1934 in the ten years preceding the date of the initial application of the Applicant/NRSRO for registration as an NRSRO or at any time thereafter?	☐	☑
B. Has the Applicant/NRSRO or any person within the Applicant/NRSRO been convicted of any crime that is punishable by imprisonment for 1 or more years, and that is not described in section 15(b)(4) of the Securities Exchange Act of 1934, or been convicted of a substantially equivalent crime by a foreign court of competent jurisdiction in the ten years preceding the date of the initial application of the Applicant/NRSRO for registration as an NRSRO or at any time thereafter?	☐	☑
C. Is any person within the Applicant/NRSRO subject to any order of the Commission barring or suspending the right of the person to be associated with an NRSRO?	☐	☑

9. Exhibits (See Instructions).

Exhibit 1. Credit ratings performance measurement statistics.

☐ Exhibit 1 is attached and made a part of this Form NRSRO.

Exhibit 2. A description of the procedures and methodologies used in determining credit ratings.

☑ Exhibit 2 is attached and made a part of Form NRSRO.

Exhibit 3. Policies or procedures adopted and implemented to prevent the misuse of material, nonpublic information.

☑ Exhibit 3 is attached and made a part of this Form NRSRO.

Exhibit 4. Organizational structure.

☑ Exhibit 4 is attached to and made a part of this Form NRSRO.

Exhibit 5. The code of ethics or a statement of the reasons why a code of ethics is not in effect.

☐ Exhibit 5 is attached to and made a part of this Form NRSRO.

Exhibit 6. Identification of conflicts of interests relating to the issuance of credit ratings.

☐ Exhibit 6 is attached to and made a part of this Form NRSRO.

Exhibit 7. Policies and procedures to address and manage conflicts of interest.

☐ Exhibit 7 is attached to and made a part of this Form NRSRO.

Exhibit 8. Certain information regarding the credit rating agency's credit analysts and credit analyst supervisors.

☐ Exhibit 8 is attached to and made a part of this Form NRSRO.

Exhibit 9. Certain information regarding the credit rating agency's designated compliance officer.

☐ Exhibit 9 is attached to and made a part of this Form NRSRO.

Exhibit 10. A list of the largest users of credit rating services by the amount of net revenue earned from the user during the fiscal year ending immediately before the date of the initial application.

☐ Exhibit 10 is attached to and made a part of this Form NRSRO.

Note: You are not required to make this Exhibit publicly available on your corporate Internet website pursuant to Exchange Act Rule 17g-1(i). You may request that the Commission keep this Exhibit confidential by marking each page "Confidential Treatment" and complying with Commission rules governing confidential treatment. The Commission will keep the information and documents in the Exhibit confidential upon request to the extent permitted by law.

Exhibit 11. Audited financial statements for each of the three fiscal or calendar years ending immediately before the date of the initial application.

☐ Exhibit 11 is attached to and made a part of this Form NRSRO.

Note: You are not required to make this Exhibit publicly available on your corporate Internet website pursuant to Exchange Act Rule 17g-1(i). You may request that the Commission keep this Exhibit confidential by marking each page "Confidential Treatment" and complying with Commission rules governing confidential treatment. The Commission will keep the information and documents in the Exhibit confidential upon request to the extent permitted by law.

Exhibit 12. Information regarding revenues for the fiscal or calendar year ending immediately before the date of the initial application.

☐ Exhibit 12 is attached to and made a part of this Form NRSRO.

Note: You are not required to make this Exhibit publicly available on your corporate Internet website pursuant to Exchange Act Rule 17g-1(i). You may request that the Commission keep this Exhibit confidential by marking each page "Confidential Treatment" and complying with Commission rules governing confidential treatment. The Commission will keep the information and documents in the Exhibit confidential upon request to the extent permitted by law.

Exhibit 13. The total and median annual compensation of credit analysts.

☐ Exhibit 13 is attached and made a part of this Form NRSRO.

Note: You are not required to make this Exhibit publicly available on your corporate Internet website pursuant to Exchange Act Rule 17g-1(i). You may request that the Commission keep this Exhibit confidential by marking each page "Confidential Treatment" and complying with Commission rules governing confidential treatment. The Commission will keep the information and documents in the Exhibit confidential upon request to the extent permitted by law.

PCR | PACIFIC CREDIT RATING

Item 3: Credit Rating Affiliates[1]

Name	Country
1. Calificadora de Riesgos Pacific Credit Rating S.A. Av. 6 de Agosto N° 2455 Edificio Hilda, Piso 9, Oficina 901, Zona Sopocachi – La Paz, Bolivia	(Bolivia)
2. Calificadora de Riesgos Pacific Credit Rating S.A. Los Dioses, San Pedro Montes de Oca Av. 10, Calle 37 Pis, 75 Norte del Bufete André Tinoco San José, Costa Rica	(Costa Rica)
3. Calificadora de Riesgo Pacific Credit Rating S.A. Av. 12 de Octubre No. 24-774 y Av. Coruña Edificio Urban plaza, segundo piso, oficina 5, Quito, Ecuador	(Ecuador)
4. Pacific Credit Rating, S.A. de C.V., Clasificadora de Riesgo Avenida la Capilla, Pasaje 8, Condominio apartamento 21 Colonia San Benito, San Salvador, El Salvador	(El Salvador)
5. Pacific Credit Rating Guatemala, S.A. Km 22,5 Carretera a El Salvador, Edificio Plaza Portal del Bosque, Torre I, Oficina 4E y 4G, Guatemala	(Guatemala)
6. Pacific Credit Rating S. A. de C.V., Clasificadora de Riesgo **Branch of Pacific Credit Rating S. A. de C.V., Clasificadora de Riesgo** Col. Lomas del Tepeyac, Avenida Las Minitas, edificio Fagar, apartamento 201A, Tegucigalpa M.D.C.	(Honduras)
7. Pacific Credit Rating S.A. de CV, Clasificadora de Riesgo **Branch of Pacific Credit Rating S. A. de C.V., Clasificadora de Riesgo (Office in El Salvador)** Avenida la Capilla, Pasaje 8, Condominio apartamento 21 Colonia San Benito, San Salvador, El Salvador	(Nicaragua)
8. Pacific Credit Rating Inc. PH Street Mall. entre Vía Brasil y Vía Israel. Piso 4. Oficina 416. Corregimiento San Francisco. Panamá	(Panamá)
9. Pacific Credit Rating (PCR), S.R.L. Calle Jacinto Mañón No. 25, Edificio Profesional JM, Piso 3, Suite 301, Ens. Paraíso, Santo Domingo de Guzmán, República Dominicana	(República Dominicana)
10. Pacific Credit Rating, USA, Inc. 2222 Ponce De Leon Blvd, Office #03-104 – 2, Coral Gables, FL 33134	(United States)

[1] All of the affiliates are separate legal entities except Nicaragua and Honduras, whose operation is conducted by the El Salvador entity. Pacific Credit Rating, USA, Inc. is a separate legal entity, wholly owned by Pacific Credit Rating Holding Inc. (Panama). Each credit rating issued by any of the affiliates is on behalf of the NRSRO: Clasificadora de Riesgo Pacific Credit Rating S.A.C. ("PCR"). Each affiliate is subject to the policies and procedures of the applicant, PCR.

Clasificadora de Riesgo Pacific Credit Rating S.A.C. ("PCR")[1]

I. Procedures and methodologies used in determining credit ratings.

II. Credit Rating Methodologies

[1]The information in this document includes all entities listed in Item 3 of PCR's Form NRSRO.

I. Procedures and methodologies used in determining credit ratings.

A. Start of Credit Ratings

The process starts with the initial contact established by the business development area with a client prospect; this contact can be in several ways: Prospect contacts PCR, PCR Country Manager contacts prospect, interested institution contacts PCR or business area identifies prospect.

The Analysis Area staff may not, for any reason, become directly or indirectly involved in the commercial and/or administrative relationship and/or rate negotiations with the prospect or with any client of the rating agency. These personnel may accompany the official in a commercial visit, with the only purpose of exposing and explaining the methodologies and criteria applied by PCR to grant a rating.

The Country Manager contacts the client and explains the PCR rating process and policies, the minimum information required to elaborate and grant a rating, and the types of rating, applicable fees, and payment policies.

Supposing the client accepts the established terms and conditions, in that case, the Country Manager proceeds to elaborate the rating services contract between the client and PCR. He asks the client for basic administrative information and a copy of the attorney's powers (s) who will sign the contract.

The Country Manager confirms with the analysis area the information required to elaborate the study, carry out the rating, and request it from the client. The Country Manager incorporates the terms and conditions of the service and payment authorized. The Country Manager prepares the invoice according to the requirements agreed with the client. He sends the contract and the invoice to the client for his signature and payment.

The client receives the signed contract and verifies that it has been signed in accordance with the agreed terms. The signature must be that of the company’s legal representative, who has sufficient authority to contract the service. The Country Manager confirms with the administration department that payment has been received from the client and generates the corresponding service order. Subsequently, the Country Manager must create the project on the PCR SI platform and share access credentials with the client.

The PCR SI Platform is the internal information management and client interaction system that centralizes the operational workflow of the analysis process, from data entry to report generation.

Unsolicited ratings

PCR may prepare unsolicited ratings. If it does so, it will only do so with public entities and issues, with the information they publish on the Stock Exchange's website or any other source of public information. The procedure and methodologies used are the same for this type of rating as for the requested ratings.

B. Rating Process

In coordination with the Senior Analyst, the Country Manager designates the Assigned Analyst and the Support Analyst for the entity's rating through the service order generated by the sales area. The analyst's selection is made considering the analysts' orientation towards economic activities, experience in similar cases, seniority in the company, and the assigned portfolio. New analysts cannot be responsible for a client until they have completed six months in PCR.

The Country Manager makes the analysts' presentation with the entity through an email. The email must be addressed to the person indicated in the service contract, who will contact the entity. The rated entity designates a contact person with whom the PCR analyst will coordinate the sending of information. The emails sent to the designated person should always be copied to the entity's direct contact (manager or responsible for the issue), who should be informed of the process's progress. Likewise, all communications should be copied to the Senior Analyst and the Country Manager.

From the first communication with the entity, the Assigned Analyst keeps an archive with all communications history. He will create a directory in the database of his mail. The record may be reviewed by the Country Manager or PCR's internal auditor.

The person responsible for instructing on the methodology to be applied for risk analysis and rating is the Quality Control Analyst. If part or all of the methodologies is not used due to an exceptional situation, a document signed by the Risk Rating Committee will be prepared, explaining the case presented and the variations applied to its methodology.

The ratings offered by PCR are opinions regarding credit quality and are not intended to suggest or encourage the purchase or sale of securities.

The information requirement for the entity or issue is prepared by the Assigned Analyst based on the information requirements defined in the risk rating operational manual. The information requirement requests both qualitative and quantitative information.

The historical financial information, if possible, should be from the last ten years (minimum three years), along with projections, investment plans, and other relevant reports to carry out the rating. In all cases, the issuer provides information on its strategies, policies, markets, finances, among others. PCR may request the information it considers relevant for the evaluation. The rating agency issues its judgment based on the analysis made of the issuer's information and other data it possesses or obtained from other sources it considers reliable to complement the documentation.

PCR ratings are developed through the strict application of its methodologies. They are based on the detailed analysis of all the information known to its analysts and considered relevant to determine a rating. This information may come from public sources, from information provided by the issuer itself or third parties; the latter are usually other companies in the same business line that have been previously rated. Because they are suppliers, competitors, or even issuer partners, they have provided information from the industry that may be useful for a correct appreciation of the rating.

The entity may send PCR additional information that it considers important for the rating process. The client must send the data within a maximum of 30 days or less, depending on the regulations in force in each country. The Assigned Analyst will review the information sent by the entity, confirming that the information requirement has complied. If information is pending, a request for information on the missing data will be made again.

To complement the entity's information in the rating or monitoring process, the Assigned Analyst will coordinate with the Senior Analyst and the Country Manager, meeting the client's different hierarchical levels. These meetings will be held with officials who have key positions in operation administration and from which it is considered relevant to gather some information. This visit is mandatory and takes place at least once a year. The Assigned Analyst must prepare a visit report, reflecting the relevant aspects

analyzed (rationality) and an executive summary, including photos, manuals, codes, and other documents provided by the entity during the visit.

The analysis process should consider the most relevant aspects for the rating and best reflect their view of the instrument or institution in the opinion of the Assigned Analyst. This analysis should cover both qualitative and quantitative aspects that support the rating issued by the analyst, including an explanation of the level of risk, for which is considered: deterioration, trends, improvements, growth, relevant facts such as acquisitions, mergers, management changes and their probable consequences, enhancements such as guarantees, taking care in evaluating the possibility of executing them and their quality. Structure in case of issues, in particular securitizations, trusts, project finance, structured. Etc.

Based on this information and the methodology, the Assigned Analyst and the Support Analyst prepare the preliminary report, which is sent to the client, without the rating proposal, to be reviewed and incorporate any comments that may contribute to the analysis.

The Assigned Analyst reviews the client's comments, and if any modification is made to the report, it is sent to the Senior Analyst for review. The Senior Analyst authorizes the Assigned Analyst to send the report to all Members of the Rating Committee.

C. Rating Committee (Committee)

The installation of the Committee shall be considered valid when at least three members or alternates are present. The presence may be physical or virtual through technological means such as video conference calls or other direct communication. The opinion of the members called to the Committee is obtained.

The Quality Control Analyst and the country's Senior Analyst are full members of the Committee. To be considered members, they must be registered in the country where the rating is made. As alternate members, Senior Analysts from other countries may participate. It is suggested that the Assigned Analysts are not Committee members. All those analysts that the Committee considers convenient to participate are considered guests. Invitees have a voice but not a vote.

The Assigned Analyst will send the presentation and the report to the Committee members with the rating recommendation at least 48 hours in advance to the convened Committee.

The Committee will be led by the Committee chair, responsible for balancing Committee members and guest participation. He will also ask for a vote from the members at the end of the exhibition.

The Committee's presentation should consider the proposed rating; the history of previous ratings; rationale and perspective; the aspects that support the analyst's opinion.

The Senior Analyst presents the case in the Committee, in which the decision of its members will establish the rating. If there are differences due to the rating in the Committee, it will be resolved by a simple majority, and in the event of a tie, the president of the Committee will have the casting vote.

Once the Committee session is concluded, the minutes will be signed, the agreements of the Committee are recorded in the minutes corresponding to that session, and the same is signed and approved by all the members of the Committee. The Senior Analyst will request the signature of the Committee members.

The approved reports will be sent by the analyst assigned to the Country Manager to communicate in writing to the representative of the issuer or entity in question, including the basis and reasoning that gave

rise to the rating. The Country Manager must also send the document to the supervisory or regulatory bodies under the country's regulations.

If the issuer or rated entity does not agree with the assigned rating. In that case, it may appeal the decision using a letter addressed to the Country Manager, provided that it can provide additional or new relevant information to PCR. The appeal and the data must be received within a period not exceeding three working days from the notification of the report's rating or receipt. PCR must respond to such an appeal within five working days. If the country's risk rating standard sets forth procedures and timeframes for the appeal and response, PCR will act following those standards.

Once the letter of appeal and the information are received within the established time frame, the Country Manager communicates with the Committee and arranges for the analysis team to review the client's information. The Senior Analyst, together with the Assigned Analyst, reviews the information and verifies that it is new and relevant to the case.

The Senior Analyst convenes the Committee 48 hours in advance, with the report reviewed by the analyst, if applicable, including new information, and at the same time prepares the presentation for the Committee. In Committee, the Assigned Analyst must present the arguments of the appeal and if the information is new or relevant.

The Committee evaluates the case and resolves the rating; this could be the initially granted ratification or a change. Once the decision has been made, the Country Manager responds to the client through a signed document and proceeds to notify the control bodies in the countries that require it and publish the information.

If the entity has a public rating contract, the Assigned Analyst prepares the press release and the executive summary. The press release must be reviewed by the Senior Analyst and validated by the Country Manager and the Quality Control Analyst.

Disclosure of information on the risk rating granted in the rating Committee will be done through a press release and the respective report on the website http://www.ratingspcr.com under the laws in force in each country concerning the publication and dissemination of information following the communications manual.

D. Public and private ratings

PCR may issue public and private ratings considering three types of private ratings:

a) Those requested by a client may be the company to rate or a third party, known as "Shadow Ratings." In these cases, the procedure and methodologies used are the same for any other rating, except for the rating information. If the client is the company itself, the rating is elaborated with the client and PCR's information, complying with PCR's minimum information requirements. Supposing the rating is requested by a third party about a public issuer. In that case, the rating is elaborated with the information that the company makes known to the investing public, unless the client requesting the rating obtains access to the issuer's data, which allows PCR analysts to have more information and to carry out possible interviews with the main officers of the company to be rated under this modality. If the company is not public, the rating is elaborated with the information that the client requestor provides, as long as it is enough to grant a rating or access the company's data.

b) Those requested by a financial institution to strengthen its internal credit and/or investment evaluation processes.

c) Those requested by a private equity investment fund to strengthen its investment process.

In no case are private ratings made public.

E. Surveillance and Monitoring

Once the rating is published, the Responsible Assigned Analyst will follow up on the rating by monitoring relevant information about the issuer and its environment on an ongoing basis. The models and criteria used to follow up the rating are the same used to determine the initial rating.

The rating is formally reviewed at least once a year with the update of the report, or earlier if necessary, according to the results experienced and under the regulations of each country.

Surveillance and monitoring activities include:

- Daily review of current news.
- Updating of sectorial information quarterly.
- Daily review of important facts of the client portfolio.

The contract for rating services indicates the quantitative and qualitative information that the issuer must report to the rating agency and the frequency with which it must do so. PCR may request additional information from the client when it considers it necessary to monitor the rating granted.

The private ratings issued will be reviewed with the periodicity specified in the rating contract, with the information specified therein. In addition to the issuer's periodic financial information, analysts must consider the issuer's relevant corporate and environmental data and include it in their review process, contacting the issuer and requesting information if they feel it necessary.

If any circumstance arises that could affect the capacity to pay or generate delays in paying obligations, the Senior Analyst must immediately call a committee and inform the Country Manager. If in an extraordinary Committee session, it is resolved to lower the rating or place it in "Review (positive or negative)," the Country Manager will inform the presidency, and the Quality Control Analyst will contact the issuer or rated entity and if necessary must inform the investing public (if the rating is public).

Rating modifications and rating review notices will be released in the same media in which they were reported, following the PCR communications manual.

Cases involving a change in rating or placing it in the review could occur when, for example:

- An issuer fails to comply with one or more of the covenants of the issue;
- That the initial characteristics of the structuring of the issue have not been fulfilled;
- That the rating agency has access to relevant information or information of public knowledge about the issuer, the entity, or its environment, or other cases that could reveal significant weaknesses.

The Committee may ratify or rectify the rating and its perspective. If it considers it relevant to the market, it may order the disclosure of the rating immediately, without prior consultation and approval of the client. The risk rating rules in force in each country must always be observed.

F. Withdraw or Suspend the Maintenance of a Credit Rating

The cancellation and/or suspension of the rating may be requested only by the issuer or by the service's contracting party. In these cases, PCR will issue a press release informing the market that it is withdrawing or suspending the rating at the issuer's express request, notifying the reasons received from the issuer and the last rating granted to this issuer.

The Technical Committee for the Evaluation of Methodologies and Rating Criteria ("The Technical Committee") may withdraw or suspend a rating if it considers that there is not sufficient and/or reliable information to maintain the rating, at the request of the Senior Analyst, who will explain the reasons for the request.

With the support of the Responsible Assigned Analyst for the issuer, the Country Manager must inform the client of the reasons for the withdrawal or suspension of the rating. If the rating is public, the withdrawal, cancellation, and/or suspension of the rating must be made public through the same means used to make it known, indicating in the statement the explicit reasons for this decision.

If the rating rules require, the regulatory body shall be informed of the rating's cancellation or suspension through an official letter.

Each press release must be published immediately on the respective decision date and must be communicated to the issuer and the regulator. Likewise, the press releases must include a link, if applicable, to the individual report and be available on PCR's website for at least 12 months from the date of publication or as indicated by the regulations in force in each country.

G. Review of Criteria and Methodologies

The Technical Committee is an independent body responsible for the rigorous and permanent revision of the methodologies and models used and the authorization of any change or modification to them.

The Technical Committee is responsible for the approval and issuance of new methodologies and models and updating these; it also accepts the annual work plan of the methodologies department.

The Technical Committee comprises at least three full members, with the entire members being: the company's executive president, who chairs the Committee, the director of analysis, and the methodology coordinator, who acts as the Committee's secretary.

The Technical Committee shall review the methodologies with a periodicity not exceeding two years to ensure their validity.

The methodologies coordinator and/or the company's executive president may call a Technical Committee meeting when they consider it necessary to review some of the methodologies or rating criteria developed by PCR.

The Country Managers will propose changes or adjustments to the methodologies and rating criteria to the methodology coordinator, who will channel them to the Technical Committee. Likewise, the Country

Managers will conduct the comments and/or proposals for improvements from the country analysts, clients, and supervisory agencies to the methodology coordinator.

The methodologies coordinator analyzes the proposals for changes or adjustments to the methodologies. If he considers that they have sufficient merit, he will call a session of the Committee in which the convenience of the proposal will be evaluated. For this purpose, he will provide the necessary information to the Committee members at least 48 hours in advance.

The Technical Committee will evaluate the information received using a wide range of measures, including statistics, to assess the performance of the credit ratings, analyze whether the methodologies should be updated, or whether the analysts' work using the methodologies should be reviewed. The methodologies coordinator discusses the new methodology, model or procedure, or modifications to the methodologies and their impact.

PCR shall report any amendments to the rating criteria and methodologies and, where appropriate, the version of any credit rating procedure or methodology used regarding a particular credit rating to the local authorities where the PCR is authorized.

PCR will also publish on its website www.ratingspcr.com any material changes to procedures and methodologies, including qualitative or quantitative inputs, the reason for the changes, and the likelihood that the changes will result in changes to any current credit rating.

PCR either changes the credit ratings that are likely to be affected by the change in methodology simultaneously with the announcement of the change in methodology or puts those ratings under review. PCR generally completes this review within six months of the announcement of the credit rating methodology update.

PCR will notify the existence of a significant error identified in a procedure or methodology, including a qualitative or quantitative model that may change the current credit ratings on its website.

II. Credit Rating Methodologies

Current versions of PCR credit rating methodologies, which are updated periodically, can be found on our website via the web address:

1	Credit Rating Methodology for Short, Medium- and Long-Term Debt Instruments, Preferred Stocks, and Issuers	www.ratingspcr.com	NRSRO
2	Credit Rating Methodology for Banks and Financial Institutions	www.ratingspcr.com	NRSRO
3	Rating methodology for provincial, municipal, and governmental entity bonds under such jurisdictions	www.ratingspcr.com	NRSRO
4	Sovereign rating methodology	www.ratingspcr.com	NRSRO
5	Risk rating methodology for holding companies	www.ratingspcr.com	NRSRO
6	Risk Rating Methodology for Non-Bank Financial Institutions or Financial Services Companies	www.ratingspcr.com	NRSRO
7	Risk Rating Methodology for Multilateral or Supranational Financial Institutions	www.ratingspcr.com	NRSRO
8	Investment Fund Risk Rating Methodology	www.ratingspcr.com	NRSRO

II. 1 Elements analyzed in the Credit Rating Methodologies:

- The strengths, weaknesses, and risks of the projects Emphasis should be placed on the probability of the occurrence of force majeure events that could alter the development of the projects and the impact that these events could have on the capacity to generate future cash flows and the payment of obligations corresponding to the investment instruments.

- The mechanisms to improve the credit quality of the investment instruments issued such as guarantees, insurance policies, collaterals, guards, among others, in order to determine the degree of protection of investors.

- The sustainability of the issuer's or project's competitive position within the industries and economic sectors they belong to.

- The nature and other characteristics of the investment projects, as well as the technical and economic solvency of its operators and any relevant element to evaluate the risk of the same. The cash flows and projected financial statements provided by the issuer, considering several possible scenarios (sensitivity analysis) and the probabilities of occurrence of each of them, including the relevant variables for the cash flow.

- Debt and liquidity policies, including guidelines for allocating assets and cash positions and policies on expenses and commissions to be paid from the fund.

- The risks associated with the fund's investment portfolio, including market, credit, liquidity, asset concentration, and quota concentration risks.

- The policies and criteria considered for the valuation of assets and management of accounting information of the assets subject to investment by the fund.

- Investment policies, taking into consideration the process of portfolio construction, instrument selection processes, portfolio diversification, restrictions by type of asset, issuer, counterparty, industry, and level of risk; restrictions on the use of options, futures, swaps, and other derivatives trading strategies; disinvestment strategies in low liquidity assets; investment tracking strategy, among others.

- The progress and general situation of the fund's activity, as well as its expectations in short and medium-term. Among the factors to be analyzed is the size of the fund, the number of participants, the financial statements, the valuation, liquidity, and the concentration of market shares. The management of the administration company is measured in terms of its experience, professional resources, organization, the definition of responsibilities and positions, support, and administration systems, to determine whether they are adequate for the fund's investment decisions.

Exhibit 3

Clasificadora de Riesgo Pacific Credit Rating S.A.C. ("PCR")[1]

- Information Security Policy
- PCR's Integrated Risk Management Manual
- Procedures for Information Security Management
- Confidentiality Agreement
- Corporate Governance Code
- Internal and Conflict of Interest Policy

[1]The information in this document includes all entities listed in Item 3 of PCR's Form NRSRO.

PCR | PACIFIC CREDIT RATING

Information Security Policy

Prepared by:	illegible signature Christian Jose Hernandez Corianga **Comprehensive Risk Management Officer** **Risks**	**Reviewed/Approved by:**	illegible signature Oscar Jasaui Sabat **Executive President**

TABLE OF CONTENTS

MODIFICATION LOG

Modification Log				
No	**Section and Page Number Modified**	**Description of change**	**Date of modification**	**Version No.**
-	Not applicable	Not applicable, as this is the first version of the document	-	1
1	Point I.7 Definitions, Page 7	Elimination of the term "CSIRT (Computer Security Incident Response Team): Team responsible for developing preventive measures and responding to computer incidents" on the grounds that PCR is not subject to regulations related to this entity.	04/21/2020	2
2	Point I.4 Legal Basis, Page 5	The Technical Standards for Information Security Management (NRP-23) are incorporated into the regulations that serve as the legal basis for this Policy	07/19/2021	3
3	Point I.5 Internal Reference Framework, Page 5	All internal regulatory documents related to this Policy are incorporated. Policy.	07/19/2021	3
4	Point I.6 Responsible parties, Page 6	This section details the responsibilities that different hierarchical levels of PCR must fulfill for proper information security management. information security.	07/19/2021	3
5	Point I.7 Definitions and Abbreviations, Pages 7-10	The meanings of the acronyms GIR, MOF, SGSI, as well as other definitions relevant to understanding the document.	07/19/2021	3
6	Point II.2 Strategies and Resources that make up the ISMS, Page 10	Details are provided on the strategies and resources used by PCR to manage information security.	07/19/2021	3
7	Point II.3 Scope of the SGSI, Page 11	The scope of the Information Security Management System (ISMS) is described. in PCR	July 19, 2021	3
8	Point III.6 Responsibility of collaborators for information security management, Page 12	The entire section III.6 is deleted, as the responsibilities of collaborators are already incorporated in point I.6 of the Policy.	07/19/2021	3
9	Point IV.3 Password management Password Management, Page 13	Clarifications are made to the password management policies .	07/19/2021	3
10	Point V.1 Reporting information security incidents, Page 14	"Any suspected cyberattack" is included in the list of incident types that PCR employees must report to the IT Analyst and the Comprehensive Risk Management Officer	07/19/2021	3
11	Point VII.4 Backups or copies of security, Page 16	Clarifications are made to the policies for backup procedures.	07/19/2021	3
12	Point I.6 Responsible parties, Pages 7 and 8	Clarifications are made to the functions to be performed by the Board of Directors, the Country Manager/Coordinator, the Chief Information Technology Officer, the Comprehensive Risk Management Officer and PCR collaborators in general.	10/28/2022	4

Log of Modifications

No	Section and Page Number Modified	Description of change	Date of modification	Version No.
13	Entire document	The positions of Head of Administration and IT Analyst are replaced by the position of Head de Technologies de la Information y Communication	October 28, 2022	4
14	Chapter IV. Access Management, Page 15	Clarifications have been made regarding the administration of user accounts and the privilege management	10/28/2022	4
15	Point VII.4 Backups or security copies	Clarifications are made regarding the responsibility of information custodians in generating backup copies. .	10/28/2022	4
16	Entire document	The position of Head of Information and Communication Technologies was replaced by Head of Information Technology	10/25/2023	5
17	Point III.8 Software Updates, Page 15	The Head of Information Technology will now be responsible for monitoring the proper updating of computer equipment every six months. Information Technology	25/10/2023	5
18	Point III.9 Return of information in the event of termination, Page 16	The Head of Information Technology is required to make backups of the digital information of officials who have left PCR. Information Technology	October 25, 2023	5
19	Point III.4 Management of confidential information, Page 13	Clarifications are made to the policies on handling confidential information	10/25/2023	5
20	Section 4. Legal Basis, page 6	Details of Peruvian regulations removed as it no longer applies to credit rating agencies	12/02/2024	6
21	Section 6. Responsible parties, pages 7-8	Adjustments were made to those responsible for compliance with this policy.	12/02/2024	6
22	Section 2, Objective, page 6	The objective was updated to include the concept of triad in Information Security.	12/03/2025	7
23	Section 4, Legal Basis, page 6	Ecuadorian regulations were added to comply compliance with the provisions of Resolution No. JPRF-T-2025-0153	12/03/2025	7
24	Section 9. Guidelines Information Security Guidelines, page 13	Information Security policies were grouped into a single section, and each guideline has been ordered according to criticality.	12/03/2025	7
25	Section 10. Report of Information Security Incidents, page 20	The "Help Desk" system was established as the official channel for reporting PCR information security incidents.	12/03/2025	7

1. BACKGROUND

All information can be considered an asset that, like any other, is fundamental to a company, so its proper safeguarding and protection is essential for the survival and continuity of business operations.

Pacific Credit Rating (PCR) is dedicated to assigning risk ratings as its main business activity, for which it handles information from various external sources (customers, stock market, economic environment, etc.) and internal sources (methodologies, analysis procedures, etc.), which leads to the need for an Information Security Policy.

2. OBJECTIVE

To establish standards and guidelines for the proper safeguarding and protection of the information that PCR generates and manages, preserving its confidentiality, integrity, availability, and reliability in accordance with defined levels and controls.

3. SCOPE

This Policy must be applied at the corporate level in all offices where PCR provides services, covering all information assets generated and managed by the organization, whether in printed or digital format.

4. LEGAL BASIS

This document was prepared in accordance with the following standards:

Country	Title of the Standard	Description
Bolivia	Compilation of Regulations for the Securities Market (ASFI)	Book 11, Title I, Chapter I: Regulations for la Gestión de Seguridad de la Information
Ecuador	Resolution No. JPRF-T-2025-0153	This document complies with the rules governing privileged, confidential, and restricted information.
El Salvador	NRP-23: Technical Standards for Comprehensive Management of Security Security of the Information	The entire document.
Other countries	No specific regulations.	In the rest of the countries, there are no specific mandatory regulations on information security for companies. .

5. INTERNAL REFERENCE FRAMEWORK

The following internal regulatory documents are directly related to PCR's Information Security Policy:

- Business Continuity Policy
- Business Continuity Plan
- Information Security Management Procedures
- Information Security Protocol

6. DEFINITIONS AND ABBREVIATIONS

a) **IRM:** Integrated Risk Management

b) **MOF:** Organization and Functions Manual

c) **ISMS:** PCR Information Security Management System

d) **Information Asset:** In information security, this refers to data, information, systems, and elements related to information technology that are valuable to PCR.

e) **Service Level Agreement (SLA):** A contract that stipulates the conditions of a service based on objective parameters, established by mutual agreement between a service provider and PCR.

f) **Information security risk analysis and assessment:** Process by which information assets, threats, and vulnerabilities to which they are exposed are identified in order to generate controls that minimize the effects of possible information security incidents.

g) **Significant Change:** Any change in the operating, IT, or business environment that has a significant influence on an Entity's risk profile.

h) **Data Processing Center (DPC)**: Physical environment classified as an exclusion area, where the resources used for information processing are located.

i) **Alternate Data Processing Center:** An alternative location equipped with computer equipment, communication equipment, workstations, communication links, power sources, and secure access, installed in a geographical location other than the Data Processing Center.

j) **Cyber threat or cyber threat:** The emergence of a potential or actual situation that could become a cyberattack.

k) **Cyberattack or cyber threat:** Organized or premeditated criminal action by one or more agents who use cyberspace services or applications or are the target of such action, or where cyberspace is the source or tool for committing a crime.

l) **Cyberspace:** A complex environment resulting from the interaction of people, software, and services on the Internet through technological devices connected to that network, which does not exist in any physical form.

m) **Cybersecurity:** The condition of being protected against physical, social, financial, emotional, occupational, psychological, educational, or other consequences resulting from failure, damage, error, accidents, harm, or any other event in cyberspace that may be considered undesirable.

n) **Encrypt:** Process by which information or files are altered, logically, including keys at the source and destination, with the aim of preventing unauthorized persons from interpreting it when viewing, copying, or using it for unauthorized activities.

o) **Password:** A set of characters that a person must enter to be recognized as an authorized user and access the resources of a computer or network.

p) **Firewall:** Device or set of devices (software and/or hardware) configured to allow, limit, encrypt, or decrypt traffic between different areas of a system, network, or networks, based on a set of rules and other criteria, so that only authorized traffic, as defined by local security policy, is permitted.

q) **Minimum information criteria:** These are the confidentiality, integrity, and availability of information.

- ✓ **Confidentiality**: Information must be kept confidential and accessible only to users who are duly authorized, trained, and supervised.
- ✓ **Availability:** Information must be accessible to authorized users when required.
- ✓ **Integrity:** Information must be complete, truthful, and accurate.

r) **Information security management:** Processes by which information security is prevented, detected, and responded to, regardless of the format of the information, including paper documents, digital and intellectual property, and verbal or visual communications.

s) **Authentication factor:** Information used to verify the identity of a service or person.

t) **Information security governance:** Set of responsibilities and practices aimed at providing strategic direction and ensuring that corporate objectives related to information security are achieved, managing it in accordance with international standards, according to the nature, size, risk profile of the entities and volume of their operations, and verifying that the company's resources are used responsibly for these purposes.

u) **Hardware:** All the physical and tangible components of a computer or electronic equipment.

v) **ISAE (Information Security Event Management) or SIEM**: Information system that provides real-time analysis of security alerts generated by applications, security devices, and network elements, such as operating system event log centralization systems.

w) **Information security incident:** An unexpected event or series of events that has a significant probability of compromising PCR operations, threatening the security of its information, and/or its technological resources.

x) **Internet:** A worldwide network of networks operating under international standards and protocols.

y) **Intranet:** Internal computer network that uses Internet technology to share information or programs;

z) Information technology infrastructure: This is the set of hardware, software, communication networks, multimedia, and other elements, as well as the site and environment that supports them, which is established for the processing of applications.

aa) Means of access to information: These are server equipment, personal computers, smartphones, ATM-type terminals, communication networks, Intranet, Internet, and telephony.

bb) *Business Continuity Plan* (*BCP*): A document that outlines the logistics to be followed by the supervised entity in order to restore critical services and applications that have been partially or totally interrupted within a predetermined time after an interruption or disaster.

cc) Least privilege principle: Establishes that each program and each user of the information system must operate using only the privileges strictly necessary to complete the work.

dd) Critical process: A process or information system that, when it stops functioning, affects the operational continuity of PCR.

ee) Data processing or system execution at an external location: Computer processes that support PCR's administrative and business operations, including: electronic card processing, mobile payment services, electronic custody of dematerialized securities in Securities Depository Entities, hosting of websites or institutional email on externally managed servers, physical hosting of servers used by the entity in external environments, and other similar processes.

ff) Information Security Program: Set of plans implemented to preserve and continuously improve information security, based on business requirements and risk analysis.

gg) Information Owner: The person formally designated to control the production, development, maintenance, use, and security of information assets.

hh) Intrusion tests: Controlled tests that identify potential weaknesses in PCR's technological resources that an intruder could exploit to gain control of its information systems, computer networks, web applications, databases, servers, and/or network devices. Intrusion tests can be performed through the internal network, from the Internet, remote access, or any other means.

ii) Resilience: the ability of a mechanism or system to recover its initial state once the disturbance to which it may have been subjected has ceased.

jj) Backup: A copy of information stored on a digital medium, generated periodically for the purpose of using that information in cases of emergency or contingency.

kk) Information security (IS): A set of measures and resources designed to safeguard and protect information, seeking to maintain its confidentiality, reliability, availability, and integrity.

ll) **Physical security**: Application of physical barriers and control procedures as preventive measures and countermeasures against threats to the entity's information assets and information.

mm) **Logical security**: application of barriers and procedures that safeguard access to information and only allow access to authorized persons or services, leaving evidence of such access.

nn) **Information system:** An organized and interrelated set of procedures for collecting, processing, transmitting, and disseminating information that interact with each other to achieve a goal.

oo) **External backup site:** An environment external to the Data Processing Center, where all backup media, documentation, and other information technology resources classified as critical and necessary to support business continuity and technological contingency plans are stored.

pp) **Software**: Equipment or logical support for an information system comprising the set of logical components that enable specific tasks to be performed. Software includes: system software, programming software, and application software.

qq) **Electronic data interchange**: A way of sending and/or receiving data, information, files, messages, and other items electronically.

rr) **Information Technology (IT)**: Set of processes and products derived from tools (hardware and software), information media, and communication channels related to the storage, processing, and transmission of information.

ss) **Outsourcing of information technology activities, operations, or processes**: Occurs when PCR entrusts the performance of information technology activities, operations, or processes related to the entity's financial services or products to a third party, i.e., a natural or legal person other than the entity.

tt) **Cybersecurity Unit (UCIB)**: Unit responsible for monitoring, evaluating, and defending the entity's information systems, such as websites, applications, databases, primary or alternate data centers, servers, networks, desktops, devices, among others.

uu) **Information system user**: Person identified, authenticated, and authorized to use an information system. This may be a PCR employee (internal information system user) or a customer (external information system user).

vv) **Vulnerability:** A weakness in an asset or control that can be exploited or used by a threat. All threats arising from the interaction of systems in cyberspace are taken into account.

7. RESPONSIBLE PARTIES

Information security management is a process that requires the commitment of all hierarchical levels of PCR, whose responsibilities are detailed below:

Instance	Responsibilities
Board of Directors	As appropriate for the country and its regulations: **a.** Approve the necessary resources for the establishment, implementation, monitoring, and maintenance of information security management, in order to have the appropriate infrastructure, methodology, tactics, and personnel. **b.** Approve the information security program or work plan each year, as well as any changes to the ISMS structure. **c.** Require Internal Audit to verify the existence and compliance of the ISMS structure.
Information Technology Committee	As appropriate for the country and its regulations: **a.** Establish PCR's strategic IT objectives and instruct the execution of tasks that will serve to optimize the use of PCR's technological resources, always taking into account the guidelines established in this Policy and in the Information Security Protocol.
Country Manager or Coordinator	As applicable to the country and its regulations: **a.** Support and ensure compliance with the information security program or work plan. **b.** Promote the continuous improvement of the ISMS and ensure its ongoing validity. **c.** Support the information security officer in the implementation of the required information security strategies and tactics. In the event of an unforeseen information security or cybersecurity incident, the Country Manager/Coordinator must report it directly to the Board of Directors or Board of Directors.
Chief Information Technology Officer	As appropriate for the country and its regulations: **a.** Perform operational tasks related to user administration and security control over logical access to PCR's various information resources. **b.** Evaluate information security and cybersecurity incidents and recommend preventive and corrective actions to the appropriate authorities, in accordance with internal procedures established by the entity.
Integrated Risk Management Officer	As appropriate for the country and its regulations: **a.** Propose to the Comprehensive Risk Management Committee the creation of specialized committees, areas, or positions to fulfill responsibilities related to information security management. **b.** Ensure that information security management is consistent with the policies and methodologies applied for risk management. **c.** Develop and propose to the Comprehensive Risk Management Committee policies and methodologies for information security management. **d.** Coordinate the administration of the ISMS between the various relevant areas of the entity. **e.** Ensure effective information security management. **f.** Propose a manual of specific information security controls to the Comprehensive Risk Management Committee for evaluation and validation, and subsequently submit it to the Board of Directors for approval, if applicable. **g.** Coordinate with the relevant areas the implementation of information security controls throughout the entity and in outsourced operations or processes related to information assets in accordance with

Instance	Responsibilities
	the classification of the information. **h.** Design and propose, to the Comprehensive Risk Management Committee for evaluation and validation, metrics that allow for the review and monitoring of information security, only if applicable. **i.** Develop awareness activities for all personnel on information security. **j.** Prepare the information security program or work plan and submit it to the Comprehensive Risk Management Committee for review, evaluation, and approval only if applicable. **k.** Inform the Risk Committee of relevant aspects of information security management for timely decision-making only if applicable. **l.** Propose the ISMS structure to the Board of Directors or Executive Committee only if applicable. **m.** Review, evaluate, and propose the information security program and resources for approval by the Board of Directors or the Executive Board. These resources must be separate from the budgets allocated to any other area of the entity. **n.** Monitor and periodically review the effectiveness of the ISMS.
Internal Audit Internal	**a.** Verify compliance with the policies, procedures, and controls implemented for the Information Security Management System.
All PCR employees	**a.** Report to their immediate superior, the Chief Information Technology Officer, and the Comprehensive Risk Management Officer any information security incidents of which they are aware, considering the details provided in the section "Reporting information security events and weaknesses" of this document. **b.** Be familiar with and understand this policy, and comply with the requirements of the PCR Information Security Protocol.

7.1 Responsible for Review and Frequency of Updates

The Comprehensive Risk Management Officer is responsible for reviewing and consequently updating or proposing the ratification of this Policy at least once a year, or when business and environmental conditions warrant it.

8. STRATEGIES AND RESOURCES THAT MAKE UP THE ISMS

PCR uses the following strategies and resources to manage information security:

1st Line of Defense

- **Users**

  All staff sign an Employment Contract and Confidentiality Agreement that outlines their obligation to protect and not disclose the information generated and managed by PCR. Similarly, the company's Organization and Functions Manual outlines the responsibility of employees to ensure the availability, integrity, and confidentiality of the information in their care.

- **Chief Information Officer**

  This department is responsible for assigning usernames and passwords to new staff and deactivating those of staff who have left the company, within the framework of the authorized access levels for each user profile.

2nd Line of Defense

- **Integrated Risk Management Officer**

  This body analyzes and evaluates the information security risks to which PCR is exposed, proposing improvements where appropriate.

- **Ethical Hacking Service Provider**

  Entity contracted to perform internal and external intrusion tests on the platforms managed by PCR, allowing the company's technical vulnerabilities to be identified.

- **Information Technology Committee**

  Body responsible for periodically monitoring and evaluating events related to information technology.

- **Information Security Officer**

  Responsible for periodically monitoring and evaluating compliance with this Policy.

Third Line of Defense

- **Internal Audit**

  Body responsible for verifying the effectiveness of the actions taken by the first and second lines of defense to achieve the objectives of the ISMS.

9. INFORMATION SECURITY GUIDELINES

9.1 Information Asset Inventory

1. PCR must establish the necessary controls to safeguard all the information it generates and manages, in accordance with the criticality levels of each asset classified in the Information Asset Inventory.
2. Information assets shall be classified according to their level of criticality (high, medium, or low) and sensitivity (confidential, internal use, public) in order to allow for the proper assignment of access rights, information owners, and responsibilities for their protection.
3. PCR must properly classify its information assets in order to define the controls it will apply to protect documentation (physical or digital) that is classified as *confidential*.
4. All owners of *confidential* information assets are responsible for requesting that the IT Department implement the controls they deem necessary to protect and safeguard such information from unauthorized persons, which may range from assigning/restricting access to specific sites, libraries, or documents on the Intranet,

to setting passwords on files or encrypting them, when deemed necessary.

9.2 Information Security Risk Analysis and Assessment

1. The Information Security Officer must perform an analysis and assessment of information security risks, in accordance with the nature, size, and complexity of PCR operations, applying the methodologies approved by the Board of Directors or Executive Committee for this purpose.
2. Among the controls mentioned, at least those implemented in computer applications for access management must be considered, as well as those that allow for the monitoring of suspicious or unauthorized activities under this Policy, including adequate records/audit trails.
3. The Internal Auditor and the Compliance area must verify compliance with the policies applied to the maintenance and operation of trading instruments, as well as the policies established in this section for the handling of confidential information.

9.3 Confidentiality Agreements

1. As part of the contractual obligations of Directors, Executives, other officers, consultants, and temporary staff, they must accept and sign the terms and conditions of the employment contract, which will establish their obligations regarding information security, including maintaining the confidentiality of the information to which they have access, even after the termination of the contractual relationship.

9.4 Information Handling

1. PCR Analysis staff may only access information on clients belonging to their assigned portfolio. To ensure compliance, the Director of Analysis must manage or request the correct assignment of access rights for all staff in their area under the *principle of least privilege*.
2. The information generated and managed by PCR must be stored on computers within individual Pacific Credit Rating OneDrive accounts, so that they have their respective replica in the cloud, which constitutes backup copies of the information, updated and synchronized in real time.
3. **Clean Desks:** PCR employees must not leave any confidential documents or working papers in view of unauthorized persons.
4. PCR personnel who do NOT belong to the Analysis department must not, under any circumstances, access the entity's client information, unless expressly authorized by the Director of Analysis or Senior Management and with due justification and a written request.
5. The methodologies, templates, and other tools that make up PCR's *know-how* must be properly safeguarded and protected by the Director of Analysis.
6. All PCR personnel are prohibited from sending or receiving confidential information through channels that are NOT authorized by the Presidency. In this regard, access to such channels must be restricted by the IT Unit to prevent their use on the computers of all Group personnel.

7. It is strictly prohibited for any PCR employee to disclose privileged information about a client or the Rating Agency itself, whether verbally, in writing, or through any audiovisual means, before such information is made public through legal and regulatory channels.
8. No PCR employee is permitted to disclose confidential data or information about the entity's clients to unauthorized persons (whether outside or within the PCR Group), whether verbally, in writing, or through any audiovisual means.
9. Rating agency staff must avoid using confidential information to participate in or otherwise influence the determination of a credit rating if they have an immediate relationship (i.e., a spouse, partner, parent, child, or sibling) who currently works for the rated entity.
10. Analysts are responsible for safeguarding and protecting information received from PCR clients (files, emails, documents, etc.), as well as internally produced documents (methodologies, templates, reports, communications, etc.).

9.5 Technical Vulnerability Analysis

1. Technical vulnerability assessments must be performed at least once (1) per year and/or when there is a significant change in the technological infrastructure, as applicable under each country's regulations.
2. The execution of security tests must consider the performance of controlled internal and external intrusion tests.
3. PCR must require companies and/or individuals that provide information security assessment services to provide the relevant documentation proving that they have the necessary experience to carry out this type of work.
4. It must be ensured that the personnel performing the controlled intrusion tests are certified and sign a confidentiality agreement as established in this Policy.
5. Identified technical vulnerabilities must be addressed in a timely manner, according to the level of risk they represent, prioritizing those that involve a high level of exposure.
6. When a vulnerability represents a high level of risk for PCR, the proposed action plan must have a maximum implementation period of 90 days.
7. Where warranted, the establishment of security patches in PCR's information systems should be considered, evaluating the risk of installing the patch versus the risk posed by the vulnerability.
8. Additionally, the following controls may be considered:
    - Disconnect or disable services or capabilities related to the vulnerability
    - Adapt or add access controls, reduce privileges
    - Increase monitoring frequency to detect or prevent actual attacks.

9.6 Controlled Destruction of Backup Media

1. To destroy backup storage media, express authorization from the Presidency must be obtained, with at least one or two of the following positions participating: Country Manager/Coordinator, Internal Auditor, or Chief Information Technology Officer.
2. All destruction of storage media must be documented in a Disposal Record, which includes: Name of the media, reason for destruction, date and time, persons responsible present, and method of destruction used.
3. Backup media may only be disposed of using methods approved by the Information Technology Department, such as degaussing, non-toxic burning, physical shredding, or secure data overwriting.
4. The use of unvalidated methods that do not guarantee the irreversibility of information recovery is prohibited.

9.7 Software Updates

1. All directors, executives, collaborators, and temporary staff who use PCR computer equipment must ensure that their operating systems and applications are properly updated.
2. The Chief Information Officer will be responsible for conducting a semi-annual review of computer equipment to verify that it is updated as appropriate and will submit a report (if necessary) on compliance or non-compliance with updates.

9.8 Return of Information in the Event of Termination

1. Any employee who terminates their employment relationship with PCR (whether through voluntary resignation or dismissal) is required to return all information in their custody during the course of their duties, accompanied by an inventory in accordance with the format in **Annex 1. Return of Information in Custody**.
2. The inventory must be signed by the employee upon delivery and by the designated official (preferably the immediate supervisor) upon receipt of the documentation.
3. The Information Technology department will make backup copies of all information on the computer equipment and OneDrive within 48 hours of the former PCR employee's departure.
4. The Information Technology department, through the Country Managers and/or Administrative Assistants, will ensure that the returned computer equipment is in good condition and ready for further use.

9.9 User Account Management

1. Access profiles must be developed for users who will access PCR's information systems and data networks.
2. The correct assignment of access profiles to users must be controlled and monitored.

3. The creation, modification, or deletion of user accounts for information systems must be authorized by the appropriate authority.
4. Access profile management must be carried out in accordance with the principle of least privilege.

9.10 Privilege Management

1. The use and assignment of privileges for user and administration accounts for information systems, applications, operating systems, databases, intranets, and the internet must be restricted and controlled.
2. When a user changes position/role within the organization, their access levels and privileges must be reassigned in accordance with the profile assigned for that purpose.
3. The access rights of users who no longer work for the company must be removed immediately.

9.11 Password Management

1. It is the responsibility of each employee to keep their passwords confidential, which means not sharing them with any other PCR employee, let alone anyone outside the organization.
2. All passwords used in PCR systems, platforms, and services must meet the minimum complexity requirements defined by the Information Technology Department.
3. Employees must change their passwords within the deadlines established by PCR and may not keep the same password beyond the maximum period determined by the Information Technology Department.
4. It is strictly prohibited to write down, store, or save passwords in visible documents, emails, chats, desktops, unprotected browsers, or any unauthorized means.
5. If the permitted limit of failed authentication attempts is exceeded, the system will automatically block the user as a preventive measure against possible unauthorized access.
6. Users' computers must be turned off or protected by a password-controlled keyboard lock when not in use.
7. If an employee detects that a colleague's computer is unlocked, they may send an email to their colleagues notifying them of the breach. The employee who breached this provision shall be subject to the established symbolic penalty, which consists of providing a snack for the team.

9.12 Backups and/or Backup Copies

1. The Chief Information Officer must monitor that all employees have their information uploaded to the cloud for proper backup when required, complying with the following minimum principles:
2. The backed-up information must have an adequate level of logical, physical, and environmental protection, depending on its level of criticality.

3. Periodic reviews must be carried out to ensure the reliability of backups in relation to their eventual use in emergencies.
4. The external backup site where the backups are stored must keep the company's critical information for at least ten (10) years.
5. The physical environment intended for the safekeeping of critical information must have sufficient physical and environmental conditions to ensure minimum protection against damage, deterioration, and theft.
6. Information custodians must maintain, at the disposal of the Information Security Officer, a repository of backup copies of highly critical information, where the name of the user and date of the last backup copy can be identified, as well as the amount of information backed up, especially in the case of information belonging to users who are former employees of the entity.
7. The Country Manager/Coordinator and/or Administrative Assistant is responsible for keeping backups of physical correspondence sent to any entity, except for those reports that the sender (Manager, Director, and/or Head) considers confidential and does not require to be archived.
8. All information generated by PCR must be stored within sites approved by Senior Management (e.g., SharePoint).

9.13 Evaluation and Selection of Information Technology Service Providers

1. The level of risk posed by a service provider to PCR must be analyzed and determined prior to hiring, and, based on the results of that analysis, the necessary controls/mitigants to be applied from the beginning to the end of the contract must be established.
2. Any contract to be signed with PCR suppliers (*Service Level Agreement – SLA*) must include, at a minimum, clauses on the type of service to be provided, the support and assistance that the provider will make available to PCR, the data security to which the provider commits, the guarantees and response times of the service (contingency/continuity plans), the availability of the service, and the penalties that will be applied in the event of non-compliance.
3. Each Country Manager/Coordinator must ensure that an up-to-date record of information on all subcontracting is maintained, including at least:
    - **a)** The name of the supplier
    - **b)** The description of the service provided to PCR
    - **c)** Start and end dates of the contractual relationship with PCR
    - **d)** Follow-up and description of any modifications or addenda made to the contract signed with the supplier

9.14 Cryptographic Controls

1. Information classified as critical and confidential by PCR must have the necessary controls in place for its protection, taking into account the option of encrypting the information when relevant, and at the discretion of the Information Owner.
2. The electronic signature option must be used for legal information when it is essential to guarantee the authenticity and non-repudiation of such information.
3. The security of information on PCR's own websites that store or transmit confidential information must be guaranteed through the use of certificates for web browsing, where appropriate.
4. If it is necessary to contract external services that require the processing of confidential data, it must be verified that data transfers are secure, either by encrypting the data before transferring it or by using secure channels.
5. If it is necessary to contract the development of a web application or mobile app that provides access to information classified as confidential, the information must be stored in encrypted form; likewise, all developers who contemplate the processing of personal data or data protected by law must consider privacy criteria by default and by design.
6. Access credentials and confidential information must be encrypted when requesting web or app developments that involve the storage, sending, or receiving of confidential information.

9.15 Information System Migration

The following policies must be applied in the event that PCR undergoes migration of its information systems:

1. Action plans must be established for the migration process, along with specific procedures to ensure the availability, integrity, and confidentiality of information.
2. The Country Manager/Coordinator is responsible for designating the entity that will perform quality control during the migration process, which must be duly documented and made available to regulatory bodies.
3. The PCR Internal Auditor must evaluate and record the results obtained from the migration process, supported by a report.

9.16 Database Administration

1. Defined architecture to organize and make the best use of information systems
2. Establishment of access controls (passwords) for confidential databases.
3. Support for administration activities (changes, modifications, debugging) of databases, subject to authorization by the owners of the information, according to the information asset inventory.
4. Conducting reviews of database capacity and performance to determine capacity expansion needs and/or timely tuning.

9.17 Software and Hardware Configuration

1. There must be a formal record containing all information relating to hardware and software configuration elements, parameters, documentation, procedures, and tools for operating, accessing, and using information systems.
2. At least once (1) a year, the existence of any personal or unauthorized software that is not included in PCR's current licensing agreements must be reviewed.
3. Equipment, operating systems, and applications must be configured in accordance with the security standards defined by the Technology Department, including minimum protection parameters, access restrictions, enabled ports, installation of corporate agents, and hardening measures.
4. The installation of any program, extension, driver, or application on institutional equipment without the prior approval of the Technology Department is strictly prohibited. All requests must be submitted through the established formal channels.
5. All ports, services, and functions that are not essential to the employee's work must be disabled on computer equipment, reducing exposure to security risks.

9.18 Training

1. All PCR employees must be trained at least once a year on this policy, information security risk management, or cybersecurity.
2. The topics covered in the training must be relevant to the employee's responsibilities and cover, as applicable, credit rating methodologies, the laws governing such rating activities, the policies applied to the maintenance and operation of trading instruments, and the policies and procedures for handling confidential or material information.
3. All new personnel joining PCR must sign their acceptance of the Information Security Policy.
4. Personnel must be trained to properly report information security incidents that may arise at PCR.

10. INFORMATION SECURITY INCIDENT REPORTING

1. All employees are responsible for reporting any information security incident as soon as possible to the Information Technology and Compliance departments.
2. The internal "Help Desk" system is the official PCR channel for recording and managing incidents. This system is administered by the Information Technology department, which must issue an initial response within a maximum of 24 hours and provide the appropriate solution within a period of no more than seven days, depending on the complexity of the case.
3. If the Information Technology department does not respond within the established time frame, the affected employee may file a complaint and/or claim with any

employee in the Compliance Department (GIR, AUI, ARG) so that the event can be followed up and a prompt response provided.

4. Any employee who fails to use the Help Desk system to report incidents or uses it improperly will be subject to the corresponding disciplinary process, in accordance with the provisions of this policy.
5. In cases of emergency, such as loss of equipment, cyberattacks, denial-of-service attacks, or loss of information due to external causes, the employee may immediately contact the Information Technology department or Comprehensive Risk Management via email, Microsoft Teams, WhatsApp, or telephone call for immediate support and assistance.

The following is a non-exhaustive list of types of incidents that PCR collaborators must report:

- Loss of service;
- Loss of equipment or facilities;
- System overload or malfunction;
- Human error;
- Non-compliance with policies or procedures;
- Deficiencies in physical security controls;
- Uncontrollable changes to the system;
- Software malfunction;
- Hardware malfunction;
- Access violations;
- Malicious code;
- Denial of service;
- Errors resulting from incomplete or outdated data;
- Violations of information confidentiality and integrity;
- Misuse of information systems;
- Successful unauthorized accesses, without visible damage to technological components;
- Recurring and non-recurring attempts at unauthorized access.
- Any suspicion of a cyberattack

11. DISCIPLINARY PROCESS

Any Director, Executive, collaborator, consultant, and/or temporary staff member of PCR who commits a breach of this Policy will be subject to the following disciplinary process:

- Verification of the occurrence of the breach by the Internal Auditor (collection of evidence).

- Review by the Compliance Department to assess the severity of the breach.
- Review of the findings of the Internal Auditor and Information Security Officer to classify the type of offense (serious, medium, minor).
- The penalties according to the type of offense are:

For Directors, Executives, employees, and temporary staff:

- Written warning with a copy added to the employee's personnel file.
- Dismissal or termination of contract, in accordance with legal regulations.

For Consultants:

- Monetary penalty monetary proportional to impact caused by the breach, and according to the contract.
- In serious cases of fraud, legal action will be considered.

12. ANNUAL IT STRATEGIC PLAN

Annually, the Chief Information Technology Officer must develop an Information Technology (IT) Strategic Plan that is aligned with the institutional strategy and considers the nature, size, and complexity of PCR's operations, its processes, structure, and analysis and evaluation of Information Security risks.

ANNEX 1. RETURN OF INFORMATION IN CUSTODY

Acta de Devolución de Información en Custodia

Yo **xxxxxxx** con número de identificación DNI **XXXXX** declaro que en fecha **21/10/2024** he realizado la devolución de la siguiente información que estuvo bajo mi custodia durante el desarrollo de mis funciones como **xxxxxx**;

Activo de Información	Título / Marca / Versión	Formato	Ubicación Electrónica o Física (ingresar dirección URL o detallar la ubicación física del activo)
Información de PCR PA, durante la gestión 2024: - ABC - XYZ - ... etc.	(Varios documentos)	Digital-Word	Carpeta(s) ubicadas en: (Ingresar link)
Laptop de 15 pulgadas	DELL Vostro 14 3000, Modelo XXXXXX, con Número de Serie 184793284928	Hardware	
Documentación de los clientes: - ABC - XYZ - ... etc.	**(Varios documentos)**	Físico	
Documentación de los clientes: - ABC - XYZ - ... etc.	**(Varios documentos)**	Digital – archivos PDF, Word, Excel.	

_____

Entregué conforme
Nombre Funcionario
Cargo Funcionario

_____

Recibí Conforme
Nombre Funcionario
Cargo Funcionario

PCR | PACIFIC CREDIT RATING

PCR's Integrated Risk Management Procedures

Prepared by:	ILLEGIBLE SIGNATURE Christian Jose Hernandez Corianga **Compliance Director**	**Reviewed / Approved by:**	ILLEGIBLE SIGNATURE Oscar Jasaui Sabat **Chief Executive Officer**

TABLE OF CONTENTS

MODIFICATION LOG

Modification log				
No.	**Section and Page No. modified**	**Description of change**	**Date of modification**	**Version**
-	Not applicable	First Version of the Document	9/4/2020	1
1	The entire document was modified	The standard is restructured at the corporate level according to the provisions of each financial system regulator in the countries where PCR provides its services. This IRM Manual is based on the principles recommended by the international standard ISO 31000:2018	31/7/2020	2
2	Section I.4 Internal Reference Framework	New regulatory documents directly related to PCR risk management are included: - Business Continuity Policy - PCR's Integrated Risk Management Procedures - PCR's Information Security Management Procedures - Information Security Protocol for the IT Unit and the GIR Area is eliminated. - Information Security Protocol for PCR Users is eliminated.	25/6/2021	3
3	Section I.5 Responsible parties, page 6.	An explanatory note is added at the bottom of the page regarding the responsibility of the Board of Directors regarding the annual subscription of the ***Declaration of Compliance*** as a regulatory requirement applicable only in PCR Peru to be sent to the SMV.	25/6/2021	3
4	Section II.7 Disclosure / Risk Communication, page 13	Reference is made to the ***Information Security Protocol***, where a list of the most common types of cybersecurity and technological risk events that must be reported to the IRM area, in case of occurrence, is displayed.	25/6/2021	3
5	Section II.8 Continuous Improvement for PCR, page 13	The role of the Integrated Risk Management area in PCR's continuous improvement process is clarified.	25/6/2021	3
6	Section I.3 Scope, page 6	Money Laundering and Terrorist Financing Risk was eliminated.	4/1/2024	4
7	Section I.4 Legal Basis, page 6	The Peruvian regulation was eliminated because as from 2023 no longer applies to Risk Rating Agencies	4/1/2024	4
8	Section I.5 Internal Normative References, page 6	The PCR Internal Reference Framework documents were updated.	4/1/2024	4
9	Section I.6.1 Responsible Compliance Officers, page 7	The Declaration of Compliance on Comprehensive Risk Management was eliminated as other mechanisms are in place in Bolivia and El Salvador to support the area compliance	4/1/2024	4
10	Section I.6.2 Responsible of Review and Periodicity Update, page 9	The term for updating this document was changed from one (1) to two (2) years.	4/1/2024	4

Modification log				
No.	**Section and Page No. modified**	**Description of change**	**Date of modification**	**Version**
11	Section II.1 Appetite, Tolerance and Capacity of Risk, page 11	Added to send the corresponding report to the Country Manager/Country Coordinator.	4/1/2024	4
12	Section II.2 Identification of Identification of Risks, page 11	LAFT Risk eliminated	4/1/2024	4
13	Section II.7.1 Senior Management, page 13	The Information Security Committee was eliminated since it no longer exists.	4/1/2024	4

CHAPTER I. GENERAL PROVISIONS

I.1 Background

The international standard ISO 31000:2018[1] describes risk management as a strategic and iterative process whose main objective is the **creation and protection of an** organization's **value**. At a specific level, ISO 31000 recommends the implementation of eight (8) principles to define the regulatory framework and risk management processes, fundamental to achieve good corporate governance:

Value creation and protection:	**Principle 1.** Risk management is an **integral part of all of the** company's **activities.** organization.
	Principle 2. A **structured and comprehensive** approach to risk management contributes to consistent and comparable results.
	Principle 3. The **risk management** framework and **process are adapted** and proportionate to the external and internal contexts of the organization related to its objectives.
	Principle 4. **Appropriate and timely involvement** of *stakeholders* allows their knowledge, views and perceptions to be considered. This results in increased awareness and informed risk management.
	Principle 5. Risks may appear, change or disappear with changes in the organization's external and internal contexts. **Risk management anticipates, detects, recognizes and responds to such changes** and events in an appropriate and timely manner.
	Principle 6. Risk management input information is based **on historical and current data, as well as future expectations**. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations.
	Principle 7. **Human behavior and culture** significantly influence all aspects of risk management at all levels and stages.
	Principle 8. Risk management is **continually improved** through learning and experience.

[1] *"Risk Management - Guidelines"* available at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

I.2 Objective of the Manual

Establish the necessary rules and guidelines to constitute an integral risk management system within Pacific Credit Rating (PCR), in accordance with the nature, size and complexity of its operations.

I.3 Scope

The company's comprehensive risk management covers the following types of risk:

1. Operational Risk (including Legal Risk and Technological Risk)
2. Information Security Risk
3. Counterparty risk
4. Liquidity Risk
5. Market Risk (Currency Risk)
6. Compliance Risk
7. Corporate Governance Risk

I.4 Legal Basis

This document complies with the guidelines established by the following rules and regulations:

Country	Title of the Standard	Description
Bolivia	Compilation of Standards for the Securities Market (ASFI), Book 11.	Article 6 of Section 3, Chapter I: Integral Risk Management, Title III, in relation to methodologies and tools for risk measurement and how these should be part of the risk management systems. risk management procedures.
El Salvador	NRP-011: Technical Standards for the Comprehensive Risk Management of Public Sector Entities. Stock Markets	Article 5, paragraph b), Article 5°, regarding the methodologies for risk measurement, and their establishment in accordance with the organizational structure, volume, nature, and levels of the company's operations. risk assumed by the company.
	NRP-023: Technical Standards for Information Security Management.	Letter a), Article 9°, corresponding to the role of the Risk Unit in the design and proposal of methodologies for information security management.
Honduras	Integrated Risk Management Standard	CBNS Circular 194/2011. Article 12, paragraph h), in connection with the revision of the of the tools y methodologies used for risk measurement and monitoring.
Rest of the countries	No specific regulations	In the rest of the countries there are no specific mandatory regulations on risk management methodologies for rating agencies/classifiers. of Risk.

I.5 Internal Normative References

The following internal policy documents are related to PCR's Integrated Risk Management Manual:

- PCR Corporate Ethics and Conduct Policy
- Information Security Policy
- Business Continuity Policy

- Business Continuity Plan
- Methodologies for Integrated Risk Management in PCR
- Regulations of the Integral Risk Management Committee (Bolivia and El Salvador)
- PCR's Integrated Risk Management Procedures

I.6 Responsible

I.6.1 Compliance Officers

Risk management is a process that requires the commitment of all the hierarchical levels of PCR, whose responsibilities are detailed below:

Instance	Responsibilities
Board of Directors	a. Establish the company's strategic objectives, evaluating and approving its strategic or business plans with due consideration of the associated risks. b. Establish PCR risk appetite and capacity. c. To know and understand all the risks inherent to the business developed by PCR, their evolution and their effects on equity levels, as well as the methodologies for risk management. d. Approve PCR's risk management policies and manuals, ensuring that they are implemented. e. Set up an Integral Risk Management area headed by a Risk Management Manager and ensure the independence of this Unit with respect to the other areas. f. Assume a proactive and preventive attitude towards risk management and ensure the effectiveness of the mechanisms for disseminating the culture of integrated risk management to all levels of the organizational structure. g. Approve the exposure limits for each type of risk, in accordance with PCR's risk appetite. Likewise, it shall establish the respective controls for exceptions and deviations to such limits, as well as the contingency plans to be adopted with respect to extreme scenarios. h. Ensure the dissemination of and compliance with policies, procedures and other regulatory documents related to integral risk management and arrange for their permanent review and updating. i. Ensure that Internal Audit verifies the existence of and compliance with the PCR risk management.
Country Manager or Coordinator	a. Implement and ensure compliance with integrated risk management and establish the corresponding preventive or corrective actions. b. Develop and implement actions leading to compliance with policies, procedures and mitigation mechanisms for the different types of risk to which PCR is exposed. c. Analyze the results obtained by PCR, considering the risks to which the company is exposed and how to mitigate them according to the regulatory framework for integrated risk management. d. Establish training and updating programs on risk management for the personnel of the Integral Risk Management area and for all those involved in operations involving risk for PCR. e. Control the implementation of methodologies for integrated risk management. f. Promote within PCR the commitment and culture of risk management. g. Allocate administrative, human and technical resources to achieve efficient risk management.
Integral Risk Management Committee	a. Ensure at all times that all personnel involved in risk management are aware of exposure limits and risk appetite. b. Design policies, systems, methodologies, models and procedures for the efficient integral management of risks. c. Analyze the risks assumed by PCR, their evolution, effects on the levels mitigation needs, additional mitigation needs and corrective actions.

Instance	Responsibilities
	d. Approve the methodologies for measuring exposures for each type of risk, and establish the possible impacts on the financial position. e. Approve the ***Annual Comprehensive Risk Management Report*** prepared by the person in charge of the IRM area, ensuring that it complies with the minimum content established by the regulatory body. f. Promote training on current regulations related to risk management for new personnel. g. Meet periodically, verifying compliance with the objectives and the results of the activities carried out by the Integral Risk Management area. h. To be aware of and follow up on the observations and recommendations made by PCR's regulatory bodies for different reasons, within the framework of their competencies. i. Approve the Annual Work Plan of the Integrated Risk Management area.
Integrated Risk Management Area	a. Develop and propose methodologies to identify and measure the different types of risks to which the company is exposed. b. Evaluate the risks to which the company is exposed, taking into account all stages of the comprehensive risk management process, in accordance with the policies and methodologies approved for this purpose. c. Ensure that comprehensive risk management considers all types of risk incurred by the company, as well as the interrelationship that may exist between them. d. Prepare an ***Annual Comprehensive Risk Management Report***, in accordance with the minimum content established by the regulatory bodies of each Country Office. e. Analyze and propose for the approval of the IRM Committee and the Board of Directors, the exposure limits and inform the Committee of the risk exposure levels. f. Implement information systems that allow adequate disclosure of risks. g. Develop a database to record risk events according to the following criteria: event identification codes, concept, type, description, amount of loss, as a minimum. h. Periodically present to the Integral Risk Management Committee the results of the activities included in its Annual Work Plan. i. Periodically monitor the company's risk profile, analyze its variations and document the causes that originated deviations from the risk exposure limits, when applicable. j. Follow up on the decisions agreed upon in the Integral Risk Management Committee. k. Efficient and timely preparation of the information required by regulators. l. Propose risk appetite, tolerance and capacity levels to the Comprehensive Risk Management Committee. m. Periodically follow up on the corrective actions presented by the units for the improvement of risk management, and bring this to the attention of the Management Committee. Integral Risk Management.
Internal Audit	a. Verify that the commercial, operational and financial areas, as well as the Comprehensive Risk Management area, have correctly executed the strategies, policies, processes and procedures approved by the Board of Directors for comprehensive risk management. b. Verify the implementation of effective internal control systems related to integrated risk management. c. Verify the correct recording of the information used for monitoring and control of integrated risk management, at least in terms of completeness, consistency, timeliness and validity. d. To review compliance with the obligations and responsibilities entrusted to the Integral Risk Management area. e. Submit reports to the Board of Directors of PCR, through its Audit Committee, on the results obtained and the suggested recommendations derived from its reviews. f. Follow-up on the observations and/or recommendations issued to the companies

Instance	Responsibilities
	different areas and communicate the results obtained to the Board of Directors, through its Audit Committee. g. Verify the documentation of the approval process of the risk measurement models, as well as their eventual modifications. h. Evaluate compliance with the policies, procedures and controls implemented for integral risk management. i. Review the organizational structure to verify the adequate segregation of duties and independence of the Integral Risk Management area.
All the officers of PCR	a. Report to their immediate superior and to the Integrated Risk Management Officer any operational risk event (including legal risk and technological risk) or information security incident of which they are aware.

I.6.2 Responsible for Review and Update Periodicity

The Comprehensive Risk Management Officer is responsible for reviewing, updating and proposing adjustments to this Manual at least once every two (2) years, or otherwise, when there are changes in the internal or external context that may affect the value of the Rating Agency.

I.7 Definitions

Internal environment: PCR's corporate culture and values; technical and moral suitability of its officers, its organizational structure and the conditions for the delegation of powers and assignment of responsibilities, among others.

Senior Management: Manager or principal executive who is part of PCR's executive staff.

Risk Appetite: The level of risk that PCR is willing to assume to achieve its objectives, within its risk capacity.

Risk Capacity: The maximum level of risk that PCR can assume without incurring regulatory non-compliance.

Control: It is the set of activities carried out with the purpose of reducing the probability of occurrence of an adverse event that may generate losses to the company.

Disclosure / Communication: Process by which the results of integrated risk management are reported to the Board of Directors and Management, as well as to *stakeholders* as appropriate.

Establishment of objectives: Process by which objectives are determined that should be in accordance with PCR's risk appetite and within its risk capacity.

Risk assessment: The process of evaluating the risks to which PCR is exposed.

exposed, using qualitative or quantitative techniques or a combination of both.

Risk Event: One or several events that may be internal or external to PCR, originating from the same cause, and occurring during the same period of time.

Comprehensive Risk Management: It is the structured, consistent and continuous process to identify, measure, monitor, control, mitigate and disclose/communicate all risks to which PCR is exposed, within the framework of a set of established strategies, objectives, policies, procedures and actions.

Risk identification: Process by which internal and external risks are identified, and which considers, as appropriate, possible events and associated scenarios.

Impact: Consequence(s) of an event that may be of internal or external origin to PCR, expressed in qualitative or quantitative terms.

Internal limit: Maximum or minimum level of exposure to a type of risk, defined internally.

Monitoring: Process that consists of the periodic evaluation of the proper functioning of integrated risk management.

Risk Exposure Level: The level of risk assumed by PCR, considering its mitigants.

Risk profile: Assessment of exposure to all types of risk assumed by PCR.

Risk response: Process by which it is decided to accept the risk, reduce the probability of occurrence, reduce the impact, transfer it totally or partially, avoid it, or a combination of the above measures, in accordance with the level of appetite and limits defined by PCR.

Risk: Probability or possibility that an event may have a negative impact on the achievement of the company's objectives, income and/or equity.

Foreign exchange risk: The probability that PCR incurs losses in its asset, liability, contingent or off-balance sheet transactions due to variations in the exchange rates of the currencies and/or units of account in which it operates.

Counterparty risk: Probability that PCR incurs losses or ceases to receive benefits due to nonpayment of obligations by its clients.

Compliance risk: Probability of incurring losses due to non-compliance with regulations and/or standards of the Financial System Supervisory Authority, the Securities Market Superintendency, the National Tax Service, or others with which PCR has regulatory obligations.

Corporate governance risk: The possibility of losses arising from failures and/or conflicts arising from the way in which the Board of Directors/Board of Directors and Senior Management relate to each other and to *stakeholders*, as well as the way in which they direct the company's activities and business.

Inherent risk: It is the risk that by its nature cannot be separated from the activity itself, being intrinsic to the processes and areas of the company, without considering the management and control systems.

Legal risk: The possibility or probability of the company incurring losses arising from non-compliance with applicable laws and regulations, or from poor contractual relationships.

This is a component of operational risk.

Liquidity risk: Probability of incurring losses from the early or forced sale of assets at unusual and/or significant discounts in order to quickly obtain the necessary resources to meet the company's obligations.

Operational or operational risk: Possibility or probability that PCR incurs losses due to internal or external fraud events, or due to failures in one of the risk factors: people, processes, systems, and external events.

Reputational risk: This risk is transversal to all the company's processes and is usually a consequence of the materialization of any of the other types of risk. Reputational risk is defined as the possibility of incurring losses as a result of the deterioration of the company's image, due to non-compliance with laws, internal rules, corporate governance codes, codes of conduct, money laundering, services rendered, technological failures, among others.

Residual risk: Risk that remains after General Management has implemented its risk response strategies.

Information security risk: Probability that a given threat will exploit the vulnerabilities of PCR's information assets, causing damage and/or loss to PCR.

Technological risk: Possibility or probability of suffering losses due to crashes or failures in computer systems, or in data transmission, programming errors or others, this being a component of operating risk.

Risk Tolerance: Acceptable level of risk to achieve a specific objective or manage a risk category.

CHAPTER II. INTEGRAL RISK MANAGEMENT POLICIES IN PCR

The bodies in charge of integral risk management (Board of Directors, IRM Committee, Senior Management and IRM area) make up the internal control environment of PCR and its corporate governance management, promoting and monitoring compliance with the rules of conduct and ethical behavior expected of all company employees as established in the *Corporate Ethics and Conduct Policy* of the PCR Group.

At a specific level, comprehensive risk management begins with the establishment of risk appetite, tolerance and capacity levels of the Country Offices, and then implementing the stages of risk identification, measurement, control, monitoring, mitigation and disclosure/communication, adaptable to the internal and external context faced by PCR.

This chapter details the policies that the Integrated Risk Management area must comply with in order to implement each stage of risk management effectively.

II.1 Risk Appetite, Risk Tolerance and Risk Capacity

The definition of PCR's risk appetite, tolerance and capacity is a fundamental piece for its risk management because it allows it to establish its objectives and limits, taking into consideration the levels of impact it is willing to assume, tolerate and reject, in search of greater profitability. These impact levels must be defined in monetary terms and/or in qualitative terms depending on the type of damage they could cause to the company.

The proposed risk appetite, tolerance and capacity levels must be submitted to the Board of Directors or Country Manager/Country Coordinator at least once every two years, including a description of the methodologies and assumptions used for the analysis.

II.2 Risk Identification

Duly supported methodologies must be defined for the identification of each type of risk, considering at least the following sources of information:

Type of Risk	Sources of information
Operational or Operational Risk (includes legal risk and technological risk)	• Process evaluation and survey interviews. • Risk event reports.
Information Security Risk	• Results of internal and external intrusion tests • Technical vulnerability reports • Information security incident reports. • User activity monitoring reports
Counterparty risk	• Treasury area reports
Liquidity Risk	• Monthly financial statements
Foreign Exchange Risk	• Evolution of Net International Reserves (NIR)
Compliance Risk	• Charge notes or notices of non-compliance by a regulator
Risk from Corporate Governance	• Institutional Strategic Plan
Reputational Risk	*Reputational risk is a transversal risk to the other risks, since it is an additional consequence related to events associated with a deterioration of PCR's image in the eyes of its stakeholders.* *stakeholders.*

	For this reason, reputational risk is identified through the management of the other risks, and is measured using the reputational risk management methodology. *operating risk.*

II.3 Risk Measurement

Duly supported methodologies must be defined for measuring risks, according to their nature, and internal limits, qualitative or quantitative scales, or a combination of both, must be applied, depending on the type of risk.

When internal limits are proposed, their analysis must be supported by an IRM Report or Report for approval by the Integrated Risk Management Committee.

II.4 Risk Control

All company processes, especially critical processes, must have adequate controls, prioritizing preventive rather than corrective actions for the treatment of potential risks.

These controls must be documented and form part of the risk analysis and evaluation performed by the IRM area.

II.5 Risk Monitoring

Risk monitoring is a periodic task that must be performed in order to follow up on the implementation of improvements in process controls. For this purpose, it is necessary to issue reports in a timely manner and to provide the necessary support to the tasks of the Integral Risk Management area.

II.6 Risk Mitigation

II.6.1 Risk Response Strategies

PCR process owners (business, administration, finance, organizational development, analysis and methodologies) as well as Country Managers/Coordinators must know their risk exposure levels in order to choose one of the following risk response strategies for risk treatment:

Level of Exhibition	Strategies for Risk Response	Description
Menor	Accepting risk	Accept the risk, without taking any action.
Under	Accept and monitor the Risk	Accept risk, but monitor it periodically.
Medium	Risk Sharing	Take actions to reduce the impact or probability of occurrence by **transferring or sharing** a portion of the risk.
High	Reduce Risk	Take actions to reduce the impact or minimize the impact the impact, the probability of occurrence, or both.
End	Risk Avoidance	Take actions to discontinue the activities that generate the risk.

Any strategy adopted must be reflected in an action plan known to the Integrated Risk Management area, with a specific timeframe for its fulfillment.

II.7 Disclosure / Risk Communication

II.7.1 Senior Management

Risks identified by the Integral Risk Management area must be disclosed to the Board of Directors through the Integral Risk Management Committee either through Reports, Reports, Risk Matrices, or others.

II.7.2 Senior Management

Where instructed by the Integrated Risk Management Committee, Country Managers/Coordinators should also be made aware of the risks to which the company is exposed, in order to facilitate the implementation of process improvements in their Country Offices.

II.7.3 PCR Collaborators

All employees must receive at least one training on integrated PCR risk management during their induction phase, when they join the company as new personnel.

Every employee is responsible for reporting any suspected or confirmed risk event to the Integrated Risk Management Officer. In case of doubts about the details to be included in their communication, they should contact the Integrated Risk Management Officer and/or the Integrated Risk Management Analyst for guidance. For events related to technological risk and information security risks, employees can refer to the list of incidents contained in the ***Information Security Protocol***.

II.8 Continuous improvement for PCR

PCR is a multi-Latin Risk Rating Company that is characterized by being at the forefront of innovation in the way it works, and this implies working on the continuous improvement of processes, systems and tools used to achieve its objectives.

Comprehensive risk management supports this practice through the recommendation of actions that prioritize prevention rather than correction of identified risks, as well as through the respective follow-up and verification of the effectiveness of the risk response plans committed to by the area leaders.

PCR | PACIFIC CREDIT RATING

Procedures for Information Security Management

Prepared by:	ILLEGIBLE SIGNATURE Christian José Hernandez Corianga **Compliance Director**	Reviewed / Approved by:	ILLEGIBLE SIGNATURE Oscar Jasaui Sabat **Chief Executive Officer**

Table of contents

MODIFICATION LOG

Modification log				
No.	**Section and Page No. modified**	**Description of change**	**Date of modification**	**Version**
-	Not applicable	First version of the document (at corporate level)	30/07/2021	1
1	Entire document	The position of IT Analyst is replaced by the position of Chief Information Technology Officer. the Information	28/10/2022	2
2	Item 5.2 Procedure for Monitoring the Activities of the Users, Page 5	The entire procedure is modified, broadening its scope.	28/10/2022	2
3	Entire document	The position of Chief of Information and Communication Technologies was replaced by Chief Technology Officer. of Information	25/10/2023	3
4	Item 5.1 Procedure for the Analysis and Evaluation of Information Security Risks, Page 4	The shipment and follow-up of the Software Inventory is clarified.	25/10/2023	3
5	Item 5.3.1 Considerations Basic, Page 7	Details of the technical support request are made through the system. "Help Desk"	25/10/2023	3

1. Target

The objective of this normative document is to define the procedures, activities and responsible parties for an effective information security management.

2. Scope

All Pacific Credit Rating (PCR) employees, temporary staff and external consultants.

3. Internal Reference Framework

The following internal policy documents are related to the Information Security Management Procedures:

- Information Security Policy
- Business Continuity Plan
- PCR's Comprehensive Risk Management Manual
- Methodologies for Integrated PCR Risk Management
- Information Security Protocol
- PCR's Integrated Risk Management Procedures

4. Responsible

4.1 Compliance Officers

They are responsible for complying with and enforcing this document:

- Country Manager/Coordinator
- Integrated Risk Management Officer
- Head of Information Technology

4.2 Reviewers and Update Periodicity

The Integrated Risk Management Officer is responsible for reviewing and consequently updating or proposing the ratification of this document at least once a year, or when business and environmental conditions warrant it.

5. Description of Procedures

5.1 Procedure for the Analysis and Evaluation of Information Security Risks

The procedure for the analysis and evaluation of information security risks aims at the identification, measurement and definition of action plans that will allow the application of an adequate treatment to such risks.

Act.	Responsible	Description
1	Officer at Risk Management Officer	Prepares and updates annually the Inventory of PCR's Information Assets, classified by their level of criticality and sensitivity. **Note:** Coordination with the owners of the information is required for the categorization of each asset.
2	Chief Technology Officer of the Information	Sends the Inventory of Software used in the company, according to format of Annex 1 of the ***Information Security Policy***.
3	Officer of Management Integral Risk Management	Follows up on the shipment of the Software Inventory to the entity. regulator.
4	Officer at Risk Management Officer	Reviews the information sent and analyzes the results of internal and external penetration tests (ethical hacking), evaluating the identified risks that may affect the company's information assets. company.

Act.	Responsible	Description
5	Officer of Management Integral Risk Management	Measures the frequency and impact of identified risks.
7	Officer at Risk Management Officer	Discloses the risks identified to the Integral Risk Management Committee, for the definition of the treatment to be applied to each one of them.
8	Committee of Risk Management Committee[1]	**Are the risks related to the misuse of passwords?** **Yes:** Its treatment is prioritized, proposing the implementation of improvements in the controls to comply with or strengthen the company's password management policies. **End.** **No:** The process continues in Activity 9.
9	Committee of Risk Management Committee	It analyzes and proposes action plans for the treatment of the identified risks, according to their level of exposure for the company. **End.**

5.2 Procedure for Monitoring Information Security Policies

The purpose of the procedure is to detect information security incidents within PCR.

Act.	Responsible	Description
1	Head of Information Technology	At least once a year, enter generate the following reports (take a random sample), and send them to the Integrated Risk Management Officer: - Logs - Azure Active Directory. - Blocked Websites Report - BitDefender. - Access Assignment Detail - SharePoint.
2	Senior Analysts	As custodians of critical information associated with a critical business activity (risk rating), they provide the IRM area, at least once a year, with the following information: - Backup copy (both physical and digital) of PCR client documentation, for a sample of at least 2 clients at random by the GIR area.
2	Officer at Risk Management Officer	Review the information provided and analyze the following: - Whether audit trails are properly configured to identify users and their activity. - If there were failed attempts to access the company's information systems. - If users are accessing only the Intranet sites/libraries that they have enabled according to their access profile - If the restriction of Internet use privileges is properly configured in BitDefender, according to the profile defined for each position. - If there were information security incidents / risk events derived from any ineffective execution of the controls implemented to safeguard the security of PCR's information. - Whether the backup copies generated by the Analysis area comply with the following: • They have an adequate level of logical, physical and environmental protection, according to their criticality.

[1] Its equivalent for PCR S.A. in Bolivia is the "Information Security Committee".

Act.	Responsible	Description
		• The physical environment for the safekeeping of critical information has sufficient physical and environmental conditions to guarantee a minimum protection against damage, deterioration and theft. • The labeling of all backup media is adequate and allows maintaining an updated inventory of backup media.
3	Officer of Management Integral Risk Management	Identifies the events or incidents that represent a risk of information security for PCR.
4	Officer at Risk Management Officer	Record critical events, if any, in the Operational Risk Event Database.
5	Officer of Management Integral Risk Management	Presents the results of the monitoring to the Integral Management Committee for the Risks.

5.3 Information Security Incident Management Procedure

The procedure is intended to ensure that information security events and weaknesses are communicated in a manner that allows timely corrective action to be taken.

5.3.1 Basic considerations

All employees should be made aware of their responsibility to report any information security event as soon as possible. In any case, the officer / temporary staff / consultant who identifies possible information security events should not take any action of their own to resolve it, without first reporting it immediately to the Head of Information Technology.

Act.	Responsible	Description
1	PCR Officer / Temporary Staff / External Consultant	During the performance of your duties, you identify one of the following information security incidents (list is not exhaustive): - Loss of service; - Loss of equipment or facilities; - System overload or malfunction; - Human error; - Non-compliance with policies or procedures; - Deficiencies in physical security controls; - Uncontrollable changes in the system; - Software malfunction; - Hardware malfunction; - Access violation; - Malicious code; - Denial of service; - Errors resulting from incomplete or outdated data; - Breaches in the confidentiality and integrity of information; - Misuse of information systems; - Successful unauthorized access, with no visible damage to technology components; - Recurrent and non-recurrent attempts at unauthorized access. - **Any suspicion of cyber-attack.**

Act.	Responsible	Description
2	PCR Officer / Temporary Staff / Consultant	Sends a technical support request through the internal "Help Desk" system to the Head of Information Technology, with all the important details of the event (type of breach or violation, bad occurred, messages on the display, description of the strange behavior).
3	Chief of Technology of the Information	Analyze the incident and evaluate possible solutions.
4	Chief of Information Technology	Can the incident be resolved remotely? **Yes:** Coordinates with the officer / temporary staff / external consultant and resolves the incident. End. **No:** Request the Administrative Assistant to contact a qualified local technician to solve the problem in coordination with the IT and Integrated Risk Management area, using for this purpose, the most effective means of communication available (Teams, Whatsapp or telephone). **Note:** If the incident is a cyber-attack, the procedures contained in the ***Business Continuity Plan*** are applied***.***

CONFIDENTIALITY AGREEMENT

In order to guarantee the confidentiality of the information, it is necessary to sign this agreement in order to guarantee levels of trust between the parties. On the one hand, **CLASIFICADORA DE RIESGO PACIFIC CREDIT RATING S.A.C.** with RUC N°**20262276407,** domiciled at Av. El Derby 254, Office 305, Urbanización El Derby, Santiago de Surco, Lima, hereinafter referred to as "**PCR",** duly represented by its Representative _____, identified with DNI N° _____y; on the other hand, _____, identified with DNI N° _____, domiciled at _____, who occupies the position of _____, who for the purposes of this act is referred to as "**THE WORKER".**

EXPOSE:

I. That **PCR** is a company whose main activity is risk rating, and , for the development of its activity, it handles privileged internal and client information, which must be handled confidentially.

II. That **PCR** includes each and every one of its subsidiaries and other related parties, both in the country and in the rest of the world, for the purposes of this Agreement.

III. That, this Confidentiality Agreement is established for the purpose of guaranteeing rigorous levels of trust between the parties and to implement the conditions under which **PCR** agrees to disclose certain confidential information, which is its property, to **THE WORKER**. The terms **PCR** and **THE WORKER** shall be understood in accordance with the provisions of the second clause of this document.

IV. That, the same shall govern the custody and non-transmission to third parties of the information distributed between the parties, as well as the rights, responsibilities and obligations inherent in the capacity of discloser and receiver of the referred information.

V. That, the parties having freely and spontaneously reached a mutual coincidence of their wills, formalize the present Confidentiality Agreement, which shall be governed by the applicable regulations and, in particular, by the following clauses.

CLAUSES:
FIRST - PURPOSE OF THE CONFIDENTIALITY AGREEMENT

The purpose of this agreement is to establish the terms and conditions under which the parties will communicate and maintain the confidentiality of the data and information exchanged between them, whether orally, graphically or in writing.

Each party hereby undertakes to treat as confidential the information that the other

party communicates to it within the framework of the collaboration, negotiations and/or projects existing between both parties. This implies that such information will receive the same treatment as confidential information of its property, and therefore, will not be disclosed to third parties, except for the exceptions provided for in this agreement.

In addition, this agreement constitutes the entire agreement between the parties with respect to confidential information and supersedes any prior understanding, oral or written, that may have existed between the parties.

SECOND - DEFINITIONS

PCR and **THE WORKER** declare and accept that it is understood and classified as "Confidential Information":

a) All information related to the activities, matters or properties obtained by **PCR** in compliance with its objective, which has become known on the occasion of the conclusion and execution of its contracts and/or within the negotiation and/or execution phases of any project related thereto, in written, verbal or visual form that has been made known to **THE WORKER** through e-mails, physical or digital documentation and/or any other means known or to be known, that is, regardless of form in which it has been received.
b) All technical, financial, accounting, legal, commercial, administrative or strategic information that constitutes a trade secret.
c) Analyses, compilations, studies or other proprietary documents or files generated from or reflecting the aforementioned information, provided that such information is not of a public nature.
d) **PCR**'s trademarks or service marks.
e) The commercial teachings of **PCR.**
f) The commercial procedures used or implemented.
g) Marketing studies contracted or prepared by **PCR.**
h) Investments held or made by **PCR.**
i) **PCR** commercial transactions**.**
j) The total or partial list of users of **PCR** services**.**
k) The total or partial list of permanent or occasional suppliers of goods and/or services acquired by **PCR** (inside and outside the country).
l) Legal controversies (judicial and/or extrajudicial) in which **PCR** is involved**.**
m) Internal control standards.
n) Commercial **PCR** files.
o) **PCR**'s personnel files and in general the private, personal and/or family information of its employees.
p) **PCR** security measures standards.

q) Likewise, all information that is marked as confidential at the time it is delivered to the other party, or from which its confidentiality is inferred due to the very nature of the information or the circumstances surrounding its disclosure, shall be considered confidential information. If there is any doubt as to the confidential nature of a particular piece of information, it shall be treated as confidential until the other party makes a determination as to its nature.

THIRD - OBLIGATIONS

THE WORKER undertakes to maintain in reserve the information classified as "Confidential Information" to which it has access on the occasion of the fulfillment of the provisions of the Employment Agreement, regardless of whether it is directly or indirectly related to its object, and therefore undertakes to:

a) Not to disclose, divulge, exhibit, show or communicate, directly or indirectly, such information in any form or by any means, at any time, either during or after the termination of the employment relationship, to any person other than its representatives or to those persons who reasonably should have access to it, without the prior written consent of **PCR**.
b) Not to use the information for purposes other than those related to the exercise and fulfillment of its obligations arising from the "Employment Contract" signed between **PCR** and **THE WORKER**.
c) **THE WORKER** undertakes to keep confidential the information related to personal data, e-mail addresses of clients, employees, shareholders and/or third parties with whom **PCR** has commercial relations and to which **THE WORKER** may have knowledge during the performance of its work.
d) The information and/or documents produced as a result of the execution of the commercial and financial objectives are the exclusive property of **PCR**. Therefore, their disclosure to third parties or even to **PCR** personnel not directly related to the execution of an analysis work, must be previously authorized by **PCR**'s management.
e) **THE WORKER** undertakes to provide the necessary means to ensure that the information is not disclosed or transferred. It will adopt the same security measures that will be adopted with respect to confidential information of its property, avoiding its loss, theft or subtraction.

FOURTH - EXCEPTIONS TO THIS AGREEMENT

Notwithstanding the provisions of this agreement, both parties agree that the obligation of confidentiality shall not apply when the information may fall under any of the following cases:

i. When the information will be found in the public domain or is classified as public.
ii. When the information was received, after its elaboration, from a third party that had the legitimate right to disclose such information.
iii. When the information has been lawfully disclosed by a third party who was under no obligation to maintain confidentiality, or
iv. When the information was independently developed by a third party without reference

to confidential information.

v. When **PCR** must deliver information classified as confidential, by order of an administrative and/or judicial authority.

FIFTH: JUDICIAL AND ADMINISTRATIVE INJUNCTION

In the event that any of the parties, their representatives or any other person to whom, within the stipulations of this Agreement, they have provided Information, is administratively or judicially required to disclose the same, the latter shall notify the other party within 48 hours of such requirement (unless expressly prohibited by law) in order to allow the adoption of the corresponding legal actions to protect their respective rights.

SIXTH - EXCLUSIVITY

THE EMPLOYEE is subject to **PCR**'s labor contract and therefore may not provide services to any other institution outside the organization, much less with companies defined as clients or competitors, taking into account that he/she may not share or use independently or personally information, formats or methodologies created or used by **PCR** during his/her permanence or at the time of termination with the organization, this clause may be grounds for a copyright lawsuit or any other type of legal action that may apply.

SEVENTH - POST-DISENGAGEMENT FOLLOW-UP

At the time of termination of **THE EMPLOYEE**, **PCR** reserves the right to carry out subsequent reviews, for a period of five (5) years from the time of termination, to determine whether the former employee joined an entity for which **PCR** had issued a qualification and to verify whether there may have been conflicts of interest on the part of the former employee that influenced at the time of granting the qualification.

In addition, if **THE EMPLOYEE** is in the above situation, he/she must notify this situation directly to the Organizational Development area of **PCR**".

EIGHTH.- DURATION OF THE AGREEMENT

This agreement is effective as of its date of signature. The parties agree that, as of said date, it shall remain in effect until 1 year after their withdrawal from the company

However, this agreement may be modified or terminated upon the express written consent of both parties.

The confidentiality provisions of this agreement shall apply for the duration of this agreement.

NINTH - RESTITUTION AND DESTRUCTION OF CONFIDENTIAL INFORMATION

In the event of expiration or termination of this agreement, regardless of its cause and within seven (7) business days following the date of such expiration or termination, you agree to

return all information and any copy thereof to the other party, insofar as it has been disclosed or transmitted on any type of media and that is its property, or if applicable, destroy it in the presence of a representative authorized by **PCR.**

In case it does not comply with the return or destruction or does not do so within the term established as required in this clause, the provisions of the eighth clause of this agreement shall apply.

TENTH - NONCOMPLIANCE

The breach of this Confidentiality Agreement shall not only result in the immediate termination of the employment contract signed between the parties, but shall also entitle **PCR** to file a civil and/or criminal lawsuit in order to establish the liabilities arising from the breach, without prejudice to our right to claim compensation for damages that such disclosure may generate.

ELEVENTH - ADDRESS FOR NOTIFICATIONS

For any notice between the parties arising out of this agreement, the parties agree that the addresses indicated at the beginning of this agreement shall be their domicile for the purpose of such notices. For a notification between the parties to be validly effected, it must be made by a reliable means that provides a record of when it was sent, to which address it was sent and the time of its receipt by the other party. When there is a change in the address for notification purposes, this new information must be communicated as soon as possible to the other party and following the procedure established herein.

TWELFTH - COMMUNICATIONS FROM PCR PERSONNEL

(a) Any PCR employee may contact the Securities and Exchange Commission (SEC) staff directly regarding a possible securities law violation.

(b) If you are a director, officer, member, agent, or employee of PCR who has an attorney, and you have initiated a communication with the Securities and Exchange Commission (SEC) regarding a possible securities law violation, the SEC staff is authorized to communicate directly with you regarding the possible securities law violation without seeking the consent of the attorney.

THIRTEENTH - LEGAL ACTIONS, APPLICABLE LAW AND JURISDICTION

The parties acknowledge that they are bound by this agreement, as well as its corresponding annexes, if any, and its legal effects, and undertake to comply with it in good faith.

Any litigation related, especially, but not only, to the formation, validity, interpretation, signature, existence, execution or termination of this agreement and, in general, to the relationship established between the parties, shall be subject to Peruvian law and shall be submitted to the courts of Lima - Peru.

The references made herein to any legal or regulatory standard or provision thereof must be understood to be made to the standards or precepts that may replace them in the future.

Thus, in case of controversy, difference, conflict or claim regarding the agreement, or in relation to the same, the parties agree, before resorting to ordinary jurisdiction, to make every effort to find an amicable solution; only when this fails, they will submit to the jurisdiction of the competent courts and tribunals according to law.

FOURTEENTH - ACCEPTANCE AND CONFORMITY

We, **PCR** through its legal representative, on the one hand, and on the other hand, **THE WORKER**, express our acceptance and conformity with each and every one of the clauses contained in this Agreement, binding ourselves to its faithful and strict compliance.

Lima, _____de 2025.

CLASIFICADORA DE RIESGO
PACIFIC CREDIT RATING S.A.C

THE WORKER

PCR | PACIFIC CREDIT RATING

Corporate Governance Code

Prepared by:	Ana Lucia Chiroy **Head of Regulatory Affairs**	**Reviewed by:**	Rafael Colado **Director of Compliance**	**Approved by:**	Oscar Jasaui **Chief Executive Officer**

TABLE OF CONTENTS

CHANGE LOG

Revision Log				
No	**Section and Page Number Modified**	**Description of Change**	**Date of Modification**	**Version No.**
1	N/A	Not applicable, as this is the first version of the document	-	01
2	Section 1, page 6	An explanation was added to the scope section	02/25/2026	02
3	Section 5, pages 6 and 7	Principles inspiring the code were added to the regulatory framework	02/25/2026	02
4	Section 7, page 7	The entity responsible for approving the code was changed to the Board of Directors	02/25/2026	02
5	Section 9, page 8	Section 9.3, "No dilution in share of the share capital"	02/25/2026	02
6	Section 10.6, pages 11 and 12	It was added that shareholders may be represented by a third party in accordance with local regulations. The proxy may be the Country Manager in accordance with the authorized representation percentage.	02/25/2026	02
7	Section 11.1, page 12	It was added that the board consists of members as defined by the regulations of each country and the Board of Directors' Bylaws.	02/25/2026	02
8	Section 11.1, page 12	The requirement that the company have alternate directors and that their information be on the website	02/25/2026	02
9	Section 11.1, page 12	It was added that the board may meet virtually if local regulations do not prohibit it	02/25/2026	02
10	Section 11.4, page 13	It was added that training for new principals will be a presentation	02/25/2026	02
11	Section 11.5, page 13	It was added that the directors will receive remuneration regardless of results/opinions.	02/25/2026	02
12	Section 11.8	The requirement that the board have a work plan and be evaluated annually	02/25/2026	02
13	Section 11.9, pages 14 and 15	Information regarding the operation , the , special , audit , and compliance, risk, and methodology committees.	02/25/2026	02
14	Section 11.10 page 15	It was added that PCR acts independently of any entity , its shareholders, directors, or related parties	02/25/2026	02
15	Section 11.12, page 16	The provision requiring the board of directors to evaluate the General Manager.	02/25/2026	02
16	Section 11.12, page 16	It was added that the objectives and everything related to Senior Management are to be found in the Company's Organization and Functions Manual, and "General Manager" was replaced with "Senior Management."	02/25/2026	02
17	Section 12.2, page 16	The provision stating that the Chief Compliance and Audit Officer be appointed by the Audit Committee.	02/25/2026	02
18	Section 12.3, page 17	It was removed that the team from audit rotate every 5 years and that the board of directors change the auditors.	02/25/2026	02
19	Section 11.9, page 14	The Internal Audit, Compliance, and Risk Committees were merged into a single committee.	04/29/2026	03

Change Log

No	Section and Page Number Modified	Description of Change	Date of Modification	Version No.
20	Section 11.9, page 14	The Committee on the Management of Complaints, Claims or Internal Complaints Management Committee was added as a special committee.	04/29/2026	03
21	Section 11.9, pages 14 and 15	The name of the Methodology Committee was changed.	04/29/2026	03
22	Section 11.9, page 15	A provision was added regarding the functional subdivision of the Internal Audit, Risk, and Compliance Committee, if required by local regulations .	04/29/2026	03
23	Section 11.9, page 15	The powers of the Committee for the Management for Internal Complaints, Claims, or Reports.	04/29/2026	03
24	Section 11.9, pages 14 and 15	The phrase “of the Company” was removed.	04/29/2026	03

1. BACKGROUND

The PCR Group (hereinafter "PCR") Corporate Governance Code is an internal regulatory document that establishes general guidelines on good corporate governance applicable to the group's companies, in accordance with current local and international standards.

It establishes a mandatory framework for conduct and decision-making for governing bodies, senior management, and all employees whose duties impact strategic direction and/or corporate governance.

2. OBJECTIVE

To establish and maintain good corporate governance practices within the company, as well as to continuously monitor the established guidelines and promote them among PCR's stakeholders.

The Code also seeks to strengthen transparency, integrity, accountability, and the long-term sustainability of the PCR Group.

3. RESPONSIBLE PARTIES

The Head of Global Regulatory Affairs and the Compliance Director will be responsible for drafting the Code and ensuring compliance with the guidelines, and must provide observations and/or recommendations aimed at promoting compliance.

4. SCOPE

This Code applies across all companies in the PCR Group, without prejudice to the specific corporate governance provisions established in each jurisdiction where the Group operates.

In countries where specific technical or regulatory standards regarding corporate governance exist, such provisions shall be considered complementary to this Code and shall prevail in the event of a conflict.

In this regard, the Code promotes, across the board, practices aimed at transparency, accountability, fairness, corporate responsibility, adequate risk management, prevention of conflicts of interest, and independence in decision-making, without prejudice to the specific provisions applicable in each jurisdiction where PCR operates.

5. REGULATORY FRAMEWORK

PCR adheres to the Principles of Corporate Governance of the Organization for Economic Cooperation and Development (OECD), originally published in 1999 and updated in 2004 and 2015 (the latest version published in conjunction with the G20). Likewise, it aligns as closely as possible with the applicable local regulations in each country regarding good corporate governance practices. These are:

- **Shareholder rights and equitable treatment**: Shareholder rights must be protected and facilitated, ensuring that all shareholders, including minority and foreign shareholders, are treated equitably.
- **Disclosure of information and transparency**: All material information about the company, including its financial condition, performance, sustainability, ownership, and governance practices, must be disclosed in a timely and accurate manner.

- **Responsibilities of the board of directors**: The board of directors must provide strategic guidance, oversee management, and be accountable to the company and its shareholders.
- **Sustainability and resilience**: Decisions and risk management that contribute to the company's long-term sustainability and resilience must be promoted.

6. DEFINITIONS

a. **Corporate Governance:** Corporate Governance is defined as the set of rules and guidelines that guide governance processes and decision-making in companies, fostering transparency and investor confidence. According to the OECD, Corporate Governance has the following characteristics: a) It encompasses a whole range of relationships between a company's management, its board, its shareholders, and other stakeholders; b) It provides a framework for the company to set objectives and determines the means that may be used to achieve those objectives and to monitor compliance; and c) It is a key element in enhancing economic efficiency and fostering growth, as well as in building investor confidence.

b. **Stakeholders:** The ISO 26000 standard defines stakeholders as individuals or groups that have an interest in any decision or activity of the organization. Similarly, the AA1000SES standard states that stakeholders are those groups that affect and/or could be affected by an organization's activities, products, or services and the associated performance. This does not include everyone who may have knowledge of or opinions about the organization.

c. **PCR Group:** This refers to companies that have PCR Holding as their primary owner, with more than a 50% equity stake. In a broader sense, it may include affiliated companies in which PCR Holding holds at least a 20% equity stake.

d. **OECD:** The Organization for Economic Cooperation and Development (OECD) comprises 38 member countries, with a mission to promote policies that improve the economic and social well-being of people around the world. The OECD provides a forum where governments can work together to share experiences and seek solutions to common problems.

7. APPROVAL AND AMENDMENT

The PCR Group's Corporate Governance Code must be reviewed by the Chief Compliance Officer and approved by the Group's Board of Directors.

8. PUBLICATION

The Corporate Governance Code document will be published on the PCR website. Likewise, in the event of any amendments to the code, the document will be updated as soon as possible.

9. SHAREHOLDER RIGHTS

9.1 Equal Treatment

- All shareholders of the same class who meet the same conditions are guaranteed equal treatment.
- The disclosure, dissemination, and use of inside information to a different group of shareholders to the detriment of the other shareholders is prohibited.
- Non-voting shares are not permitted.

9.2 Shareholder Participation

- All shareholders have the opportunity to participate effectively and to vote at general meetings of shareholders, for which they are informed in a timely manner of the rules governing such meetings, including voting procedures.
- The company informs shareholders of the methods and the entity responsible for registering share ownership rights.

9.3 Information and Communication to Shareholders

- Shareholders have the right to request and receive timely, reliable, and accurate information regarding the company's activities, which enables them to adequately safeguard their rights.
- The body designated to handle specific requests for information from shareholders is the Board of Directors, or, in its absence, the Country Manager, who may delegate the handling of such requests to other persons.
- Shareholders may submit requests for information in person, in writing, by phone, or via email. The designated department must respond to the shareholder using the same methods indicated above, specifying the approximate time required to respond to the request. All information provided must meet criteria of accuracy, completeness, timeliness, and non-discrimination.

9.4 Dividend Policy

- The company has a formally approved dividend policy, which is reviewed and updated periodically.
- The dividend policy is disseminated to shareholders and investors and is available upon request.

9.5 Change of Control

- Anti-takeover mechanisms are not promoted.
- In the case of tender offers, shareholders are recognized and enabled to participate in the premium paid to acquire control of the company.

9.6 Dispute resolution

- The bylaws include an arbitration clause that provides that any dispute between shareholders, or between shareholders and the Board of Directors, shall be submitted to arbitration, as well as

Challenges to resolutions of the General Shareholders' Meeting and the Board of Directors by the company's shareholders.

10. GENERAL MEETING OF SHAREHOLDERS

10.1 Role and Authority

- The General Shareholders' Meeting (GSM) is the sovereign and supreme body of the company.
- The exclusive and non-delegable functions of the GSM are stipulated in the Bylaws and in the current regulatory framework.

Likewise, the GSM must perform strategic functions necessary to ensure the achievement of objectives and goals, such as defining strategic objectives, corporate strategies, and action plans; monitoring levels of exposure to risks related to the achievement of objectives; supervising expenses and investments; ensuring budget compliance; and overseeing corporate governance practices and investment policy, among other functions.

10.2 Shareholders' Rights and Responsibilities

- As holders of the Company's equity capital, shareholders have a set of rights and duties that are essential to the proper functioning of the Company and the protection of its interests, in accordance with current regulations and the principles of good corporate governance. These include, among others:
    - Registering and safeguarding their ownership rights through reliable mechanisms.
    - Disposing of, assigning, or transferring their shares in accordance with applicable legal and statutory provisions.
    - Authorizing the issuance of new shares or any modification to the share capital, under the terms set forth in the bylaws.
    - Participating in the distribution of profits in accordance with their shareholding and the decisions adopted by the shareholders.
    - Receiving, in a timely and sufficient manner, relevant, verifiable, and understandable information regarding the Company's financial, operational, environmental, and social performance.
    - Elect and remove, as appropriate, members of the Board of Directors, including its chairman, ensuring the suitability, independence, and diversity of its composition.
    - Approve, amend, or repeal the Company's governing documents, including the bylaws and internal regulations.
    - To decide on significant transactions that may involve a major structural change, such as the disposal of strategic assets or mergers and acquisitions.
    - Determine or approve the compensation policy for members of the Board of Directors and senior management.

- Approve the appointment of the external auditor and oversee, through the Board of Directors, the independence of said auditor.
- To be informed in a timely manner of the rules governing the operation of General Shareholders' Meetings, including procedures for deliberation, voting, and representation.
- To receive, with sufficient advance notice, clear and sufficient information regarding the date, time, location, format (in-person, virtual, or hybrid), required quorum, agenda, and supporting documents related to the matters to be discussed at any General Shareholders' Meeting.
- To participate and exercise their right to vote effectively and without any restrictions at any General Shareholders' Meeting, whether in person or remotely, with identical legal effects.

10.3 Convening Procedures

- The General Shareholders' Meeting must be convened with due notice and in strict compliance with the procedures established by the bylaws and applicable legal provisions. It must be convened at least once per fiscal year, preferably during the first quarter.
- The annual shareholders' meeting shall be deemed validly constituted if it has the quorum provided for in the bylaws; failing that, it may be held by universal consent with the presence and unanimous consent of the shareholders entitled to vote, provided that this is permitted under applicable corporate law.
- The notice of meeting specifies the place, date, and time of the general meeting, as well as the matters to be discussed (agenda). The notice may also include the place, date, and time at which, if necessary, the general meeting will be held on second call. Such a second meeting must be held no earlier than three days and no later than ten days after the first.
- The general meeting may not address matters other than those specified in the notice of meeting, except in cases permitted by law.

10.4 Proposals for Agenda Items

- Any shareholder may request the inclusion on the agenda of the General Shareholders' Meeting of matters of corporate interest that fall within the legal or statutory jurisdiction of the Meeting.
- The interested shareholder must submit a written request or an email addressed to the Chairman of the Board of Directors, specifically indicating the items they request to be included on the agenda and the appropriate justification for each case.
- To this end, the company provides shareholders with sample letters they may use, which are optional; shareholders may use other formats provided they include the items mentioned in the preceding paragraph and the applicant's contact information (name or business name of the shareholder, telephone number, and email address).

- The Board of Directors must review the requests and communicate its decision to the interested shareholder within a maximum of ten (10) business days after receiving the request. Such communication shall be made using the means described above. If the Board of Directors denies the request, it must explain the reason for its decision.

- With regard to requests to include items on the agenda of the Mandatory Annual Meeting, such requests may be submitted by February 15 of each year. Notwithstanding the foregoing, shareholders may submit their requests throughout the year, which will be evaluated following the same procedure described herein; however, acceptance of such requests does not imply that the Board of Directors must call a General Shareholders' Meeting to address the matter. In this regard, matters included in requests that have been accepted by the Board of Directors will be included on the agenda of the next General Shareholders' Meeting, should the Board decide to convene one during the course of the year, or, otherwise, on the agenda of the next Mandatory Annual Shareholders' Meeting.

10.5 Voting Procedures

- The general guidelines for the exercise of voting rights at meetings by shareholders or their representatives are set forth in the bylaws.

- Shareholders shall have the option, if they deem it necessary, to vote separately on matters that are substantially independent, so that they may exercise their voting rights separately. This rule shall apply in particular to the appointment or ratification of directors (which must be voted on individually) and to amendments to the bylaws (for each article or group of articles that are substantially independent).

- Additionally, the company has established mechanisms that allow shareholders to cast their votes remotely through secure electronic or postal means, and that ensure the person casting the vote is indeed the shareholder.

- The company allows those acting on behalf of multiple shareholders to cast separate votes for each shareholder, so as to comply with the instructions of each principal.

10.6 Proxy Voting

- Shareholders entitled to attend the meeting may be represented by another shareholder or by a third party, without any restrictions and in accordance with the provisions of the applicable local regulations.

- The power of attorney must be granted by any means of communication that leaves a written record and specifically for each meeting, except in the case of powers of attorney granted by public deed, which must be registered no later than 24 hours prior to the time set for the meeting.

- Shares held by legal entities shall be represented at General Meetings by the Country Manager or by duly authorized representatives for that purpose.

- The company provides shareholders with a proxy form template, which includes the representatives' details, the matters for which the shareholder delegates their vote, the authorized percentage of representation, and, where applicable, the direction of their vote for each proposal.

10.7 Follow-up on Resolutions of the General Shareholders' Meeting

- For the purpose of monitoring the resolutions adopted by the General Shareholders' Meeting, the Board of Directors appoints a person responsible for performing this function, who may be a director, the Country Manager, or any other officer designated by the Board of Directors.
- In addition, the designated individual must submit periodic reports to the Board of Directors on the progress of the implementation of the resolutions adopted at the Annual General Meeting.

10.8 Equal Treatment of Shareholders

The Company recognizes the equitable treatment of all shareholders holding shares with equal rights as a guiding principle of good corporate governance. Accordingly:

- Equal conditions are guaranteed regarding access to information and participation in relevant decisions.
- The dissemination of privileged or asymmetric information that grants undue advantages to one or more shareholders is prohibited.
- The rights of minority shareholders are protected against potential abusive practices, such as:
- Transfers of value to related parties without economic justification.
- Transactions not aligned with the company's interests.
- Changes in the shareholding structure that unjustifiably favor certain shareholders.

Likewise, institutional mechanisms will be made available to channel complaints, claims, or alerts regarding potential infringements on shareholders' rights, ensuring their proper handling and resolution.

11. THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT

11.1 Composition of the Board of Directors

- The minimum and maximum number of directors shall be in accordance with the applicable local regulations of each country and as specified in the Board of Directors' Bylaws.
- The participation of independent directors will be encouraged to strengthen objectivity in decision-making.
- To the extent possible, the Board of Directors shall be composed of individuals with diverse expertise and skills, who possess prestige, ethical standards, financial independence, sufficient availability, and other qualities relevant to the company, so as to ensure a plurality of perspectives and opinions.
- The Board may meet virtually if local regulations do not prohibit it.

11.2 Duties of the Board of Directors

- The functions of the Board of Directors are established in the Articles of Incorporation and the Board of Directors' Bylaws.
- Notwithstanding the foregoing, the Board of Directors is also responsible for approving and directing the company's corporate strategy; establishing objectives, goals, and action plans, including annual budgets and business plans; overseeing and supervising management; and managing the company's governance and administration.
- The Board of Directors oversees good corporate governance practices and establishes the policies and measures necessary for their optimal implementation.

11.3 Specialized Advisory Services for Decision-Making

- Directors have the right to request the support or input of experts in cases requiring specialized advice for decision-making.
- The individual or firm providing the advice must have recognized prestige and a proven track record in the market.
- Furthermore, if the decision is of a technical or highly specialized nature, it must be verified that the advisor holds the required certifications in the relevant field.

11.4 Training Policy for the Board of Directors

- The company offers an orientation program for new directors. The training will consist of a presentation during which participants will be informed about the company's activities and the responsibilities of the position. In addition, new directors must receive the key regulations and guidelines with which they are required to comply.
- The company also has an ongoing professional development program for directors. This program includes a series of training sessions on specific topics identified as relevant to enhancing directors' decision-making.

11.5 Compensation for Directors

- The position of director will be compensated regardless of results and/or opinions expressed.
- For each Board meeting, directors receive a fixed per diem, in accordance with the conditions and characteristics stipulated in the Bylaws.
- The Annual General Meeting, in its mandatory annual session, must approve the amounts of directors' per diems for each fiscal year.

11.6 Board of Directors Bylaws

- The company shall have formally approved Board Regulations.
- This document contains the policies and procedures for its operation, its organizational structure, as well as the duties and responsibilities of the Chairman of the Board.
- It is binding, and failure to comply with it entails liability.

11.7 Independent directors

- Independent directors are those who have no ties to the company, its major shareholders, or its executives.
- They are selected based on their professional background, experience, specific expertise, and financial independence.

11.8 Board Operations

- The company has established mechanisms that allow directors to participate in meetings remotely, either via videoconference or conference call.
- Notice of Board meetings must be issued by the Chairman or the person designated by him, within the timeframes and under the conditions set forth in the Bylaws. This notice must be sent via certified mail, fax, email, or other similar means of communication, provided that a written record is maintained in each case, and must be issued no later than five (5) days prior to the date set for the meeting.
- The notice must specify the location, date, and time of the meeting, as well as the items to be discussed.
- The notice may be waived when all directors meet and unanimously agree to hold the meeting and discuss the agenda items.
- Information regarding the agenda items listed in the notice must be made available to the directors on the same day the notice is issued. The information may be sent to the directors in physical or electronic format. Additionally, such information is made available to shareholders at the company's principal office.

11.9 Special Committees

- The Board of Directors has three support committees: a) Internal Audit, Risk, and Compliance Committee; b) Internal Complaints, Claims, and Allegations Management Committee; and c) Technical Committee for the Evaluation of Methodologies and Rating Criteria. These constitute technical support bodies for the Board of Directors and do not replace its non-delegable responsibilities. All Committees act with functional independence, report directly to the Board of Directors, and submit their conclusions, reports, and recommendations to the Board for the corresponding decision-making.
- The Internal Audit, Risk, and Compliance Committee shall meet as necessary to fulfill its functions and at least once a year, or as required by local regulations in each jurisdiction, to draft proposals for changes to PCR's internal regulations resulting from:
    - Changes in regulations
    - Improvements to internal processes
    - Recommendations resulting from regulatory inspections
    - Identification of areas for improvement

- The Internal Audit, Risk, and Compliance Committee is composed of the Chief Compliance Officer, the Internal Auditor, and the Chief Risk Officer; however, if the jurisdiction of each country specifies a different composition and/or requires the committee to be subdivided for the purpose of functional separation, the latter shall be followed, in which case the committees shall be formed separately. A quorum shall be met when at least a majority of the total members are present, provided that the Chief Compliance Officer is always present.

- Additionally, the committee may meet as necessary to fulfill its duties and at least once a year, or as required by the local regulations of each jurisdiction, to evaluate situations in which the rating agency's independence and impartiality could be compromised.

- The Internal Complaints, Claims, and Allegations Management Committee is composed of the Chief Compliance Officer, the Chief Risk Officer, and the Head of Organizational Development. The Committee is responsible for monitoring complaints and claims from qualified entities, analysts, investors, and the general public, which will be addressed in order to analyze their root causes, track their progress, resolve them, and communicate the results. If the matter concerns one of the members, they will be replaced on the Committee by an alternate member.

- The Internal Complaints, Claims, and Reports Management Committee will address internal complaints, claims, and/or reports within a maximum of fifteen (15) business days; it will determine the course of action for the internal complaint, claim, or report and instruct the responsible party to respond with the Committee's resolution, as well as the PCR areas affected by that measure.

- The Technical Committee for the Evaluation of Rating Methodologies and Criteria will meet annually and will be responsible for reviewing, discussing, and agreeing upon the Institution's rating methodologies and any modifications thereto, as well as the quantitative models incorporated into those methodologies and the criteria for their application.

- The Technical Committee for the Evaluation of Methodologies and Qualification Criteria is composed of senior management from the Analysis Department. A quorum shall be met when at least a majority of its total members are present, provided that the Director(s) of Analysis must always be present.

- Likewise, other employees may be appointed as members of the three committees, depending on the nature of their position, knowledge, and duties.

11.10 Ethics and Conflict of Interest Policy

- PCR acts with full technical, operational, and discretionary independence with respect to issuing companies and other entities subject to rating. Rating decisions are made objectively, impartially, and autonomously, without undue influence from economic, commercial, financial, or any other interests linked to the rated entities, their shareholders, managers, or related parties.

- Compliance with independence standards is governed by the formally approved Ethics Policy, which applies to all staff, including directors and senior executives.
- This document, along with other guidelines, defines situations involving conflicts of interest and the specific procedures for their prevention, detection, management, and disclosure.
- During the induction program for new directors, they receive a copy of the Ethics Policy and are trained on compliance with it, with particular emphasis on the situations in which a conflict of interest could arise.
- The company designates a person responsible for monitoring compliance with the Ethics Policy, who must submit periodic reports to the Board of Directors.
- Formal channels have been established so that employees or any member of the public may file complaints regarding non-compliance with the Ethics Policy, especially in cases of conflicts of interest.

11.11 Transactions with Related Parties

- The company has a policy for the valuation, approval, and disclosure of transactions with related parties, including transactions with companies within the economic group.
- This policy includes the criteria for determining related party status, the valuation procedures, and the guidelines for the approval and disclosure of transactions with related parties.

11.12 Functions of Senior Management

- The functions, objectives, and all matters related to Senior Management are defined in the company's Organizational and Functions Manual. Likewise, the functions of the Chairman of the Board of Directors are defined in the Board of Directors' Bylaws.
- Senior Management shall be appointed or replaced by the board of directors or the shareholders.
- The positions of Senior Management and Chairman of the Board of Directors are held by different individuals, ensuring a clear separation between the company's management and the Board of Directors.
- The total annual compensation for Senior Management includes a variable component, which takes into account the achievement of previously defined strategic objectives and the efficient management of risks.

12. RISK AND COMPLIANCE

12.1 Comprehensive Risk Management Policy

- The company has a comprehensive risk management policy, approved by the Board of Directors and applicable to the entire business group.
- The Country Manager periodically monitors risk levels and overall compliance with the guidelines set forth in the aforementioned policy, issuing reports to the Board of Directors.

12.2 Internal Audit

- The Compliance Officer and the Head of Internal Audit perform compliance and audit duties exclusively; they possess autonomy, experience, and expertise in the matters under their evaluation, as well as independence to monitor and assess the effectiveness of the risk management system.
- The internal audit function may be performed by company personnel or by external personnel. In both cases, the internal auditor must observe the principles of diligence, loyalty, and confidentiality required of the Board of Directors and Senior Management.

12.3 External Audit

- The General Shareholders' Meeting, upon the Board of Directors' proposal, appoints the auditing firm or independent auditor responsible for conducting the external audit of the company's financial information.

13. TRANSPARENCY OF INFORMATION

13.1 Information Policy

- The company has an approved confidentiality agreement that defines the general guidelines for the handling, collection, preparation, classification, organization, and/or distribution of information generated or received by the company.
- The Board of Directors periodically monitors compliance with the information policy.
- The Country Manager is responsible for responding to requests for information from the company's various stakeholders, including shareholders, investors, the local community, the government, and the media, among others.

13.2 Financial Statements and Annual Report

- The company prepares its financial statements in accordance with the International Financial Reporting Standards (IFRS) in effect as of the date of issuance by the International Accounting Standards Board (IASB).
- Likewise, upon the Board of Directors' proposal, the General Shareholders' Meeting approves the company's annual report, which is distributed to its main stakeholders.

14. STAKEHOLDER ENGAGEMENT

14.1 Identification of Stakeholders

- As part of its sustainability policy, the company has a formally approved stakeholder identification procedure through which it identifies stakeholders' expectations regarding the company's activities.
- This procedure is updated periodically, taking into account the inclusion of new stakeholders or changes in their expectations.

14.2 Strategies for engaging with stakeholders

Taking into account the identified stakeholders and their specific expectations, the company defines specific engagement strategies for each of them.

PCR | PACIFIC CREDIT RATING

Internal Policy and Conflict of Interest Policy

Prepared by:	Illegible signature Christian Jose Hernandez Corianga	**Reviewed by:**	Illegible signature Rafael Colado Ibarreche	**Approved by:**	Illegible signature Oscar Martin Jasaui Sabat
	Head of Risk Management		**Director Compliance**		**Position / Title**

TABLE OF CONTENTS

MODIFICATION LOG

Log of Modifications				
No	**Section and Page No. Modified**	**Description of change**	**Date of modification**	**No. of version**
1	Not applicable	First version of the document	09/04/2024	1
2	Section 5, Basic considerations page 6	A paragraph was included with information on how to avoid conflicts of interest PCR staff	01/15/2025	2
3	Appendices 1 and 2, pages 21 and 22	The Affidavit for PCR directors, officers, and employees and the form for handling potential conflicts of interest by PCR personnel were included. PCR staff	January 15, 2025	2
4	Section 8. Internal control structure, page 16	A diagram showing the structure of the internal control system has been added.	05/06/2025	3
5	Section 9. Follow-up after termination of executives and technical staff (look back review), page 16	It added the procedure for employee separation (look back review)	05/06/2025	3
6	Annexes 3 and 4, pages 23 and 24	Two annexes were included containing a table of penalties and the procedure for manage potential conflicts of interest.	05/06/2025	3
7	Section 4. Definitions, page 5	New definitions related to SEC authorization were included.	02/03/2026	4
8	Section 5 Basic considerations Basic considerations, page 6	A paragraph was included with the types of conflict of interest.	03/02/2026	4
9	Section 12. Compensation Compensation Policy, page 18	A section containing the Compliance and Risk Compensation Policy has been included.	03/02/2026	4
10	Section 13. Policy on Internal Investigations, page 18	A section containing the Policy for conducting internal investigations was included.	03/02/2026	4
11	Section 14. Procedure for the publication of global ratings overall grades, page 19	A section was included that contains the procedure for publication publication of overall grades	02/03/2026	4
12	Section 15. Submission of information to the SEC, page 20	A section was included containing the information that must be submitted to the SEC in a regulatory manner	03/02/2026	4
13	Annex 5, page 25	An annex was included containing the list of information that must be kept in PCR.	03/02/2026	4
14	Annex 6 Procedure for determining publication of format 17g7, page 28	Annex 6 Procedure for determining the publication of the format was included. 17g7	03/02/2026	4
15	Annex 7 Schedule for regulatory filing with the SEC, page 29	Annex 7, Regulatory filing schedule with the SEC, was included.	02/03/2026	4

1. OBJECTIVE

To establish guidelines that Pacific Credit Rating (hereinafter PCR) personnel must follow to identify, prevent, and avoid conflicts of interest inside and outside the company, in order to ensure transparency, integrity, and impartiality in the performance of their daily activities.

2. SCOPE

This document applies to all PCR employees, including directors, committees, or anyone involved in the risk rating activities carried out by the company.

3. RESPONSIBLE

3.1 Compliance

All personnel, according to their position at PCR, must comply with and enforce this policy, with emphasis on the following areas:

- **Management:** Ensure that company personnel avoid engaging in acts of conflict of interest.
- **Administration and Finance:** Protect the company's interests by avoiding conflicts of interest both internally (permanent or temporary staff) and externally (suppliers).
- **Organizational Development:** Prevent actions or activities that generate conflicts of interest with staff in general. The area has internal processes for recruitment and selection of personnel, hiring and induction of personnel, training and development, evaluation and performance, termination of personnel, and a conflict of interest clause in the employment contract.
- **Comprehensive Risk Management:** Identifies, assesses, and manages risks associated with conflicts of interest. Annually manages an Annual Risk Plan and ensures that all employees complete the affidavit for directors, officers, and employees of PCR, as well as the PCR personal conflict of interest form.
- **Audit:** Evaluates PCR processes with an independent perspective in order to manage compliance with this policy. An Annual Audit Plan is carried out each year and the Internal Audit Manual is reviewed every two years.

3.2 Communication and Updates

The compliance area, with the support of the Comprehensive Risk Management Officer, is responsible for communicating this policy and making the corresponding updates as appropriate, or rectifying it within a period of no more than two (2) years.

4. DEFINITIONS

a. Conf**lict of Interest:** Any situation as a result of which a natural or legal person may obtain advantages or benefits for themselves or for third parties, and which affects their independence when making decisions.

b. **Independence:** This implies that the functions performed by an area or individual may be exercised freely, in the absence of conflict of interest, minimizing through processes the interaction with areas potentially affected in their respective functions and with the aim of being able to exercise these functions with their own resources, impartially, independently, and without external influences.

c. **Ethics and conduct policy:** Set of rules governing the behavior of the entity and its employees; expressing its commitment to ethical values and principles such as transparency, good faith in business or activities, compliance with current legislation and the entity's policies, as well as fair treatment of customers who are in the same objective conditions. It includes, among other things, the explicit prohibition of behavior that could give rise to reputational risks or improper or illegal activity, such as the reporting of incorrect financial information, money laundering and terrorist financing, fraud, anti-competitive practices, bribery, corruption, and the violation of customer rights.

d. **Transparency:** All technical processes, from their administration and control, are open to public review, to users in general, control and regulatory bodies, and to other participants in the securities market.

e. **U.S. Securities and Exchange Commission (SEC):** The U.S. Securities and Exchange Commission is a government agency whose function is to supervise securities trading in U.S. markets.

f. **Nationally recognized statistical rating organization (NRSRO):** A nationally recognized rating organization in the United States.

g. **The NRSRO form:** This is the application for registration to become a Nationally Recognized Statistical Rating Organization in the United States.

h. **Code of Federal Regulations (CFR):** The United States Code of Federal Regulations.

i. **Electronic Data Gathering, Analysis, and Retrieval (EDGAR):** A system that provides free public access to millions of informational documents filed by publicly traded companies and other entities in the United States.

j. **Employment Transition Report**: Report submitted to the SEC when an analyst or executive changes jobs.

5. BASIC CONSIDERATIONS

For PCR, implementing an institutional ethics process is particularly important because of the significant impact that trust and transparency have on relationships with customers, investors, regulators, and the general public.

Therefore, prevention activities have been designed and established to address any potential conflicts of interest that may arise, as well as different channels for reporting them.

5.1 Prohibitions

All persons who are part of PCR are prohibited from having conflicts of interest in relation to the issuance or maintenance of a risk rating.

A person within PCR is considered to be the Rating Agency, its credit rating subsidiaries, and any partner, officer, director, branch manager, and employee of the organization.

PCR is prohibited from the following:

1. Making the issuance of a rating conditional on or threatening to make it conditional on the purchase by the rated person, or an affiliate thereof, of any other service or product.
2. Issuing or maintaining a rating requested by a person who, in the most recent fiscal year, provided the Rating Agency with net income equal to or greater than 10% of the organization's total net income for the fiscal year.
3. A person within PCR buying, selling, or otherwise benefiting from any transaction in securities or market instruments when the person has knowledge of material non-public information.
4. That a person involved in determining or monitoring the risk rating, or in developing or approving the procedures or methodologies used to determine the credit rating, engages in sales or marketing activities for a product or service of the organization or is influenced by sales or marketing considerations.
5. Hiring persons who provide or have provided financial advisory, consulting, or auditing services for the client's financial statements within the twelve (12) months prior to the rating.
6. Hiring individuals who have spouses and/or relatives up to the second degree of consanguinity or affinity who are related to a client.
7. Hiring individuals who directly or indirectly hold securities issued by the client or have received securities issued by the client as collateral.
8. Hiring individuals who have pending legal proceedings against them with any of the supervised entities or with the financial system, depending on their country.
9. Hiring individuals who have participated in illegal or unauthorized financial activities in the securities market and financial system, depending on their country.
10. Hiring individuals with whom there is a conflict of interest, litigation, or outstanding debts with the client.
11. Hiring individuals who have been convicted of crimes committed in the incorporation, operation, or liquidation of companies or for other common crimes, up to five (5) years after having served their sentence.
12. They may not be part of the Board of Directors or the executive or operational staff of clients with whom PCR has a risk rating contract.
13. They shall not perform consulting work or make recommendations, directly or indirectly, for companies with which PCR has a risk rating contract.
14. They shall not hold any direct or indirect title to securities issued by the client.
15. They may not receive any benefit from any PCR client.

16. Under no circumstances may they directly or indirectly acquire securities that have been rated by themselves.
17. The segregation or delegation of functions between employees from different areas is prohibited.
18. Under no circumstances may it offer a client advantages, incentives, compensation, or indemnification of any kind that could be detrimental to others or to market transparency.
19. The inappropriate dissemination, inside or outside the organization, of material non-public information obtained in connection with the provision of risk rating services is prohibited.

All PCR employees are subject to compliance with the following general aspects:

20. They will be subject to audits or verification in the performance of their duties when required or requested by the Compliance, Audit, or Risk areas.
21. At least once a year, ~~they shall sign~~ the "Affidavit for directors, officers, and PCR employees" of no conflict of interest at PCR, in order to continue performing their duties.
22. All employees must report the existence of conflicts of interest. This can be done through secure and confidential reporting channels that guarantee privacy and trust among employees, which may be anonymous and external, protecting the whistleblower from retaliation and ensuring a fair investigation.
23. PCR must conduct reviews to determine whether there could have been conflicts of interest on the part of a former employee who influenced the granting of a rating. (Look back review).
24. The areas of Comprehensive Risk Management, Internal Audit, and Compliance are independent and will act as a control function in all PCR processes and will make improvements as appropriate to the processes, based on previous findings.
25. The acceptance of any type of gifts, currency, favors, or benefits from entities with which there is any type of contract or relationship is prohibited.
26. Any gifts, currency, presents, or benefits must be reported within a maximum of 48 hours to a manager in the areas of Comprehensive Risk Management, Internal Audit, and Compliance.

PCR conducts training programs so that PCR employees can identify and disclose any potential conflicts of interest.

PCR shall prepare and/or maintain all information necessary to account for the provision of rating services, business activities, and regulatory compliance issues. The information shall be retained for a period of at least five years; however, certain specific documentation shall be retained for an additional period of five years.

All PCR directors, officers, and employees must submit the declaration contained in **Annex 1, "Affidavit for PCR Directors, Officers, and Employees," and** the form contained in **Annex 2, "PCR Personal Conflict of Interest Form,"** related to situations that could give rise to a conflict of interest.

Failure to comply with any of the above provisions may result in disciplinary measures as indicated in **Annex 3, "Table of Sanctions**."

In the event that any PCR employee fails to disclose in a timely manner any situation that could give rise to a conflict of interest, or conceals such a situation, the case will be analyzed by the Compliance Department, in conjunction with the Institution's General Management, with the opinion of the Board of Directors, and the measures to be applied will be determined, in accordance with the provisions of **Annex 3 "Table of Sanctions."**

The handling of potential conflicts of interest shall be carried out in accordance with the flowchart contained in **Annex 4, "Handling of Potential Conflicts of Interest."**

PCR has identified the following types of conflicts of interest related to the issuance of credit ratings as potentially significant for its activity.

1. PCR receives payments from issuers or underwriters to determine credit ratings for securities or money market instruments that they issue or underwrite.
2. PCR receives payments from clients to determine their credit ratings.
3. Issuers, underwriters, or debtors who have paid PCR to determine a credit rating may pay for services additional to the determination of credit ratings.
4. PCR allows individuals who are part of the company to directly own certain securities or money market instruments of debtors or issuers subject to a credit rating determined by PCR, or to have other direct interests in them, provided that such individuals do not participate in the determination or approval of the credit rating.
5. PCR may provide ancillary services such as reviews and ratings of corporate governance, social responsibility, and fiduciary duty.

6. SPECIFIC CONSIDERATIONS

Without prejudice to the previous section, the specific considerations for each area that must be complied with are detailed below.

6.1 Board of Directors

1. The members of the Board of Directors are appointed and/or removed by the Shareholders' Meeting, and there must be no fewer than three members. Decision-making is carried out democratically by majority vote. The presence of all or a majority of its members constitutes a sufficient quorum to deliberate and make valid decisions.
2. The members of the Board of Directors have a Chairman, a Vice Chairman, and a Secretary, who shall exercise the powers conferred upon them by the Institution's bylaws.
3. PCR maintains a policy that at least half of the members of the Board of Directors, but no fewer than two of its members, must be independent. The term of office of independent directors shall be for a fixed period agreed in advance, which shall not exceed five years, and shall not be renewable. One of its independent directors must be a user of PCR ratings. The provisions of this paragraph shall be applicable in accordance with the laws of each country.
4. It is the body responsible for electing the members of the Rating Committee, as well as for approving, supervising the establishment, maintenance, and application of policies and

procedures for determining credit ratings. The provisions of this paragraph shall apply in accordance with the laws of each country.

5. No member shall be part of the Board of Directors if they have a conflict of interest that prevents them from performing their duties objectively and independently.
6. They shall have the time and effort necessary to fulfill their responsibilities.
7. They shall supervise the establishment, maintenance, and application of policies and procedures to address, manage, and disclose any conflicts of interest.
8. They shall oversee the effectiveness of the internal control system.
9. They shall appoint the Chief Compliance Officer, the communications officer, and the complaints officer.
10. You must approve:
    - The annual compliance report.
    - The procedures and methodologies, including qualitative and quantitative data and models, that PCR uses to determine risk ratings.
    - The results of executive look-back reviews.
    - The results of compliance and risk audits.
    - The complaint handling report.
    - The employee compensation and promotion policy.
    - The analysis area report on PCR methodologies.
    - The company's financial statements.
    - Documents that form part of PCR's internal regulations, which include the Corporate Ethics and Conduct Policy and its amendments.
    - The organization's compensation and promotion policies and practices.

6.2 Rating Committee

1. No employee or external party shall be part of the Qualification Committee when they are in a position to take actions or make decisions that directly benefit them or, failing that, that benefit related third parties and that such actions or decisions conflict with the interests of the company.
2. If the members of the Qualification Committee detect or identify a conflict of interest with respect to a specific issue, the person involved must withdraw and leave, including physically, the discussions and deliberations, without neglecting their legal duties.
3. There should be no political or economic pressure from the client or other entities arising from the capital structure, commercial or financial activities, or interests of members and clients.
4. Any member of the Qualification Committee, regardless of country, shall be dismissed when any of the circumstances that determine the existence of a conflict of interest or causes of disqualification and incompatibility arise, or when they are declared legally incompetent.

6.3 General Management

1. It shall establish an organizational structure with a clear segregation of commercial and analytical functions.
2. Responsible for monitoring compliance with PCR's goals and objectives, satisfying the Board of Directors with responsible management of the entire organization, adequately planning resources, and reporting on the progress of its goals and objectives. Responsible for directing, coordinating, and administering the general operation of the Institution.
3. Together with the Director of Compliance and Risk, it shall be aware of any situation that could generate a potential conflict of interest with respect to the granting of a rating to an entity and participate in the imposition of measures to manage such conflicts.
4. The General Management is not authorized to conclude that the PCR internal control system is effective at the end of the fiscal year if there are one or more material weaknesses in that system at the end of the fiscal year.
5. It may not use confidential information obtained through its position for personal gain or for the benefit of third parties.

6.4 Analysis Area

1. No analyst shall be a member of the Rating Committee of their country without prior authorization or availability for action in accordance with the regulations of their country.
2. No employee in the analysis department shall have a commercial relationship with the client.
3. They shall not condition or threaten to condition the issuance of a rating on the purchase by the client or a related company of any other service or product.
4. They shall not assure or guarantee a rating in advance of the corresponding evaluation by the Analysis Committee and the publication of the rating.
5. Their spouses and/or relatives within the second degree of consanguinity and second degree of affinity may not be clients or participants of the supervised entities in which they perform such functions.
6. Any update to an analysis document or corporate methodology must be communicated to all staff in a timely manner within a period not exceeding 15 days through a channel authorized by PCR, in addition to providing the corresponding training. Additionally, the following will be published on the website:
    - Substantial changes in procedures and methodologies, including qualitative models or quantitative data used to determine credit ratings.
    - The reason for the changes and the likelihood that they will result in changes to current credit ratings;
    - Notification of the existence of a significant error identified in any procedure or methodology, including a qualitative or quantitative model used to determine credit ratings, which may result in a change in current credit ratings.

6.5 Business Area

1. Warn customers or whomever is appropriate about conflicts of interest that may arise in the course of providing the risk rating service.
2. Avoid establishing personal relationships with customers that could compromise commercial objectivity.
3. Any contract signed with a potential PCR client may be reviewed in advance by the Head of Global Affairs or a legal control area.
4. Establish strict parameters between the business and analysis areas in order to avoid influences on the risk rating processes.
5. It is prohibited to conduct business or commercial agreements on behalf of the company in unofficial settings or outside of established channels.
6. No Country Manager or Coordinator may offer the service if they are involved in litigation against the subject of the rating or the contracting entity, its affiliates, related parties, or subsidiaries.

6.6 Comprehensive Risk Management Area

1. This area must be independent from all other areas of PCR in order to avoid conflicts of interest and ensure an adequate separation of responsibilities.
2. It will assess and determine situations in which the independence and impartiality of the rating agency is affected, either ex officio or at the request of an interested party.
3. It shall promote a culture of risk and ethics throughout PCR, emphasizing compliance with the processes defined in each manual.
4. It shall develop and monitor, together with the Compliance Director, policies and procedures for the handling of non-public information to avoid conflicts of interest.
5. Be aware of reports of gifts from PCR employees.
6. Request acknowledgments of acceptance of the Corporate Ethics and Conduct Policy.
7. Ensure reasonable compliance with ethical business conduct and maintain effective control against potential conflicts of interest.
8. Conduct periodic reviews to verify compliance with internal regulations by managers and employees.
9. Monitor complaints and grievances from qualified entities, analysts, investors, and the general public regarding ratings, models, methodologies, policies, and procedures.
10. Design policies and procedures for efficient comprehensive risk management
11. The Risk Management Officer's compensation shall not be linked to the financial results of the Rating Agency and shall be carried out in such a way as to guarantee the independence of the officer's judgment.
12. The Risk Management Officer may not perform credit ratings, marketing or sales functions, or participate in the establishment of compensation levels.

6.7 Internal Audit Area

1. This area must be independent from all other areas of the CRA in order to avoid conflicts of interest and ensure an adequate separation of responsibilities.
2. Evaluate and determine situations in which the independence and impartiality of the rating agency is affected, either ex officio or at the request of an interested party.
3. Work with the Compliance Director and the Risk Management Officer to identify any situation that could generate a potential conflict of interest with respect to the granting of a rating to an entity and participate in the imposition of measures to manage such conflicts.
4. Maintain an impartial and neutral attitude and avoid any conflict of interest.
5. Communicate in a timely manner any conflicts of interest, limitations on scope, restrictions on access to records, personnel, and assets, and limitations on resources such as financial resources to senior management and the audit committee.

6.8 Compliance Area

1. Monitor compliance with regulations applicable to securities rating agencies and the proper functioning of the internal control system.
2. It must be independent from all areas of PCR in order to avoid conflicts of interest and ensure an adequate separation of responsibilities.
3. Assess and determine situations in which the independence and impartiality of the rating agency is affected, either ex officio or at the request of an interested party.
4. Prepare the annual compliance report, which includes:
    - A description of any significant changes in the Corporate Ethics and Conduct Policy and in the policies for handling conflicts of interest.
    - A certification that the report is accurate and complete.
    - Submit the report to the Board of Directors for approval.
5. Be informed about reports of gifts by PCR employees.
6. Be aware of reports to avoid conflicts of interest and reports of illegal or unethical conduct, situations, or activities submitted by employees.
7. Prepare annual reports and regulatory reports.
8. Assess and determine situations in which the independence and impartiality of the rating agency is affected, either ex officio or at the request of an interested party.
9. Prepare and monitor, together with the Risk Management Officer, policies and procedures for handling non-public information and avoiding conflicts of interest.
10. Conduct post-termination monitoring of executives (look back review).
11. Conduct periodic reviews to verify compliance with internal regulations by managers and employees.
12. Verify that regulatory reports have been submitted in a timely manner.

13. Monitor complaints and grievances from rated entities, analysts, investors, and the general public regarding ratings, models, methodologies, policies, and procedures.
14. Oversee and monitor the internal control system.
15. The Compensation of the Compliance Officer shall not be linked to the financial results of the Rating Agency and shall be carried out in such a way as to guarantee the independence of the officer's judgment.
16. The Compliance Director may not perform credit ratings, marketing or sales functions, or participate in the establishment of compensation levels.

The General Compliance Department shall maintain an up-to-date log of persons who present a potential conflict of interest with any of the entities rated by PCR.

The General Compliance Department shall keep a record of gifts offered to PCR personnel.

7. CONTROL SYSTEM

With regard to the establishment of the control system, PCR will take into consideration the following controls, designed to ensure:

1. A newly developed methodology or a proposed update to a methodology in use for determining credit ratings is subject to an appropriate review process.
2. Methodologies in use for determining credit ratings are reviewed periodically.
3. That newly developed or updated quantitative models proposed for incorporation into a credit rating methodology are evaluated and validated prior to use.
4. Quantitative models incorporated into credit rating methodologies in use are periodically reviewed and tested.
5. That the Rating Agency conducts an analysis before initiating the rating of a class of debtors, securities, or market instruments that it has not previously rated, in order to determine whether the rating agency has sufficient expertise, access to the necessary information, and resources to rate the type of debtor, security, or market instrument.
6. That the Rating Agency conduct an analysis before initiating the rating of an "exotic" or "customized" type of debtor, security, or market instrument, in order to review the feasibility of determining a risk rating. Likewise, those business activities that are classified as high risk according to GAFILAT.
7. That measures (e.g., statistics) be used to evaluate the performance of risk ratings as part of the review of methodologies in use to determine risk ratings, in order to analyze whether methodologies need to be updated or whether the work of analysts using them needs to be reviewed.
8. That a risk analyst document the steps taken in preparing an initial credit rating or monitoring an existing credit rating in sufficient detail to allow for a post-hoc review or internal audit of the rating file,

in order to analyze whether the analyst complied with the Rating Agency's procedures and methodologies for determining credit ratings.

9. That the Rating Agency conduct periodic reviews or internal audits of rating files to analyze whether analysts adhere to the procedures and methodologies of the nationally recognized statistical rating organization and determine credit ratings; and finally.

10. That the Rating Agency conduct periodic reviews to verify whether it has devoted sufficient resources to implement and operate the documented internal control structure as designed; (more on the internal control structure below)

11. That the Rating Agency conduct periodic reviews or continuous monitoring to assess the effectiveness of the control structure and whether it needs to be updated;

12. That any deficiencies identified in the internal control structure be evaluated and addressed in a timely manner, for which the Comprehensive Risk Management area has a Risk Matrix.

13. That additional training be provided or disciplinary measures be taken with respect to employees who do not comply with the requirements imposed by the internal control system;

14. That there is a process for employees to report breaches of the control system.

15. PCR must have an Internal Audit Observations Report to ensure that any deficiencies identified in the internal control system are evaluated and addressed in a timely manner.

16. To assess the effectiveness of internal control, the Executive President or CEO will determine whether there were any material weaknesses based on the annual results of the audits performed by the Compliance area.

17. The results of the evaluation of the analysis control system shall be documented in the internal control report. This report must be approved by the Board of Directors and shall contain at least the following:

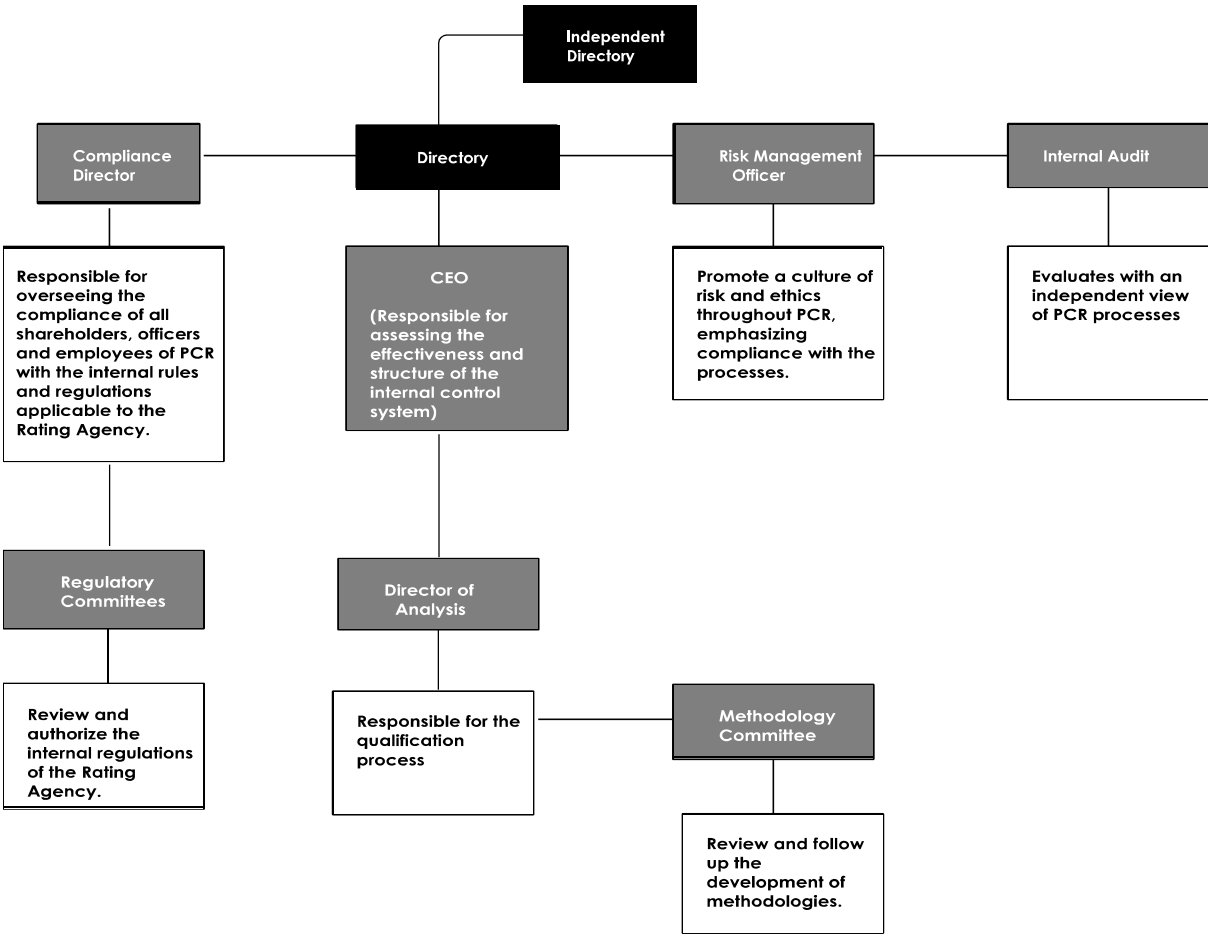
- A description of management's responsibility for establishing and maintaining an effective internal control structure;
- A description of each material weakness in the internal control structure identified during the fiscal year, if any, and a description, if applicable, of how each material weakness identified was addressed; and
- A statement as to whether the internal control structure was effective at the end of the fiscal year.

18. The Chief Executive Officer shall not conclude that PCR's internal control system is effective at the end of the fiscal year if there are one or more material weaknesses in that system at the end of the fiscal year. For purposes of this item, a deficiency in the internal control system occurs **when the design or operation of a control does not enable management or employees, in the normal course of performing their assigned duties, to prevent or detect a failure of the organization to:**

- Implement a policy, procedure, or methodology to determine credit ratings in accordance with the organization's policies and procedures; or
- Adhere to an implemented policy, procedure, or methodology for determining credit ratings.

For the purposes of this section, a material weakness exists **if** a **deficiency** or **combination of deficiencies** in the design or operation of the control system **creates a reasonable possibility that an identified failure** (as described in the previous paragraph of this section) that is material **will not be prevented or detected in a timely manner**.

8. INTERNAL CONTROL STRUCTURE



9. POST-TERMINATION FOLLOW-UP OF EXECUTIVES AND TECHNICAL STAFF (LOOK BACK REVIEW)

PCR must carry out reviews through the Compliance Department to determine whether there could have been conflicts of interest on the part of a former employee who influenced the granting of a rating.

In the event that, within five (5) years of leaving PCR, a former employee joins an entity for which PCR has issued a rating, the following procedure must be carried out to rule out any possible conflict of interest on the part of the former employee with the company they have joined:

1. Notification of the Organizational Development area where a former employee, who was an analyst who participated in any way in determining the rating of the entity, issuer, or instruments, or the analyst's supervisor or a PCR executive, has been hired by an entity that is a PCR client within five (5) years of leaving PCR.

   The Compliance Director analyzes whether any of the following three conditions are met:

   - The former employee was a manager.
   - If the former employee participated in any way in the rating process of the entity where they are providing their services.
   - If the former employee supervised an analyst who participated in any way in the rating process of the entity in which he or she is providing services.

2. If any of these criteria are met, the Employment Transition Report is submitted through the SEC website.

3. As soon as the Chief Compliance Officer becomes aware of the former employee's entry into the entity, the ratings assigned to that entity will be reviewed for the 12-month period prior to the date on which PCR issued the most recent rating action with respect to the entity, taken before the employee's departure. This is established to verify that there has been no potential conflict of interest.

4. If there's any evidence that the rating was influenced by a conflict of interest, a rating review process should be started, which will take 15 calendar days. PCR will publish the rating change or confirmation of the rating, as applicable, within fifteen calendar days of the date on which it was detected that the rating may have been influenced by a conflict of interest.

   If the rating change or confirmation of the rating is not published within the period specified in the previous paragraph, PCR must issue a press release stating that the rating is under review or observation because evidence was found that the rating may have been influenced by a conflict of interest.

10. ATTENTION TO COMPLAINTS AND CLAIMS

Complaints and claims from customers and relevant related parties will be handled through the complaints, claims, and reports mailbox located on the Intranet in the Comprehensive Risk Management section. Additionally, through the rating agency's website in the "Complaints Mailbox" section.

11. DOCUMENTATION OF INFORMATION

PCR shall maintain all necessary information regarding the provision of rating services, business activities, and financial matters in general. In general terms, the information shall be retained for a period of at least five years, although certain specific documentation shall be retained for an additional period of five years.

The list of documents that must be retained in accordance with Rule 17g-2 of the Code of Federal Regulations ("SEC Rule") is set forth in **Annex 5 "List of information to be prepared and maintained at PCR"** of this Policy.

12. COMPENSATION POLICY

12.1 Remuneration

The remuneration of the board of directors, management and technical staff involved in the rating process, and employees in general, shall be determined in accordance with a fixed component that is not related to the ratings issued by the Rating Agency or its income. The remuneration of all employees shall also take into account the annual performance evaluations administered by the Organizational Development Department.

Remuneration policies and structures for management and technical staff will be reviewed periodically to ensure that the objectivity of the rating process is not compromised.

12.2 Compliance Area

The Compliance area reports directly to the Board of Directors. The salaries of the staff assigned to this department are not related in any way to the income received by the rating agency for its ratings and are determined in such a way as to guarantee the independence of its criteria.

12.3 Risk Area

The Risk area reports directly to the Board of Directors, and the salaries of the staff assigned to this department are not related in any way to the ratings issued by the rating agency. The Risk staff will submit an annual report on its activities to the Board of Directors.

13. POLICY ON INTERNAL INVESTIGATIONS

When, as a result of its oversight functions, or based on a report submitted by an employee or manager of the Institution, the Compliance area becomes aware of a violation by an employee or manager of applicable regulations or of a situation that could give rise to a conflict of interest, it shall conduct an investigation, recording such conduct or situation in a follow-up log.

The Compliance Director will give the person involved the opportunity to verbally state what is in their best interest, which must be recorded in the tracking log.

Measures to resolve potential conflicts of interest will be decided by the Compliance and Risk area, in conjunction with Senior Management.

Sanctions will be applied taking into consideration **Annex 3 "Table of Sanctions"** of this Policy. However, the sanction may be mitigated if the offender admits to having committed the offense and, where appropriate, has remedied the breach in question.

The sanctions or measures imposed must be recorded in the monitoring log, which must include any information that has been taken into account in determining the sanction.

14. PROCEDURE FOR THE PUBLICATION OF OVERALL RATINGS

14.1 Overall ratings

In the case of global ratings, the business area must ask the client whether the securities offering is directed at a "US person" as defined below, in which case the form of SEC Rule 17g7(a) must be used as described in **Annex 6 "Procedure for determining the publication of Form 17g7 (a)(1).** A written statement must be obtained from the client indicating whether or not the offering is directed at a US person.

US person:

1. Any natural person residing in the United States;
2. Any company or corporation organized or incorporated under the laws of the United States;
3. Any estate whose executor or administrator is a U.S. person;
4. Any trust whose trustee is a U.S. person;
5. Any agency or branch of a foreign entity located in the United States;
6. Any non-discretionary account or similar account (other than an estate or trust) held by a dealer or other fiduciary for the benefit or account of a U.S. person;
7. Any discretionary account or similar account (other than an estate or trust) held by a dealer or other fiduciary organized, incorporated, or (if an individual) resident in the United States; and
8. Any partnership or corporation if:
    a. Organized or incorporated under the laws of any foreign jurisdiction; and
    b. Formed by a U.S. person primarily for the purpose of investing in securities not registered under the Act, unless it is organized or incorporated and owned by accredited investors who are not individuals, estates, or trusts.

Additionally, for global ratings, the analyst must review, in accordance with the definitions detailed below, whether Rule 144A is mentioned in the Securities Offering Prospectus or Offering Memo, or if the issuer intends to sell the security to a US person, as described in Annex I "Information Disclosure Form for Global Ratings" of this policy.

14.2 Prospectus

It is a legal and financial document that a company must submit before a public offering of securities. Its purpose is to provide investors with all relevant corporate, legal, and financial information so that they can make an informed investment decision. This document details the characteristics of the company and the securities to be sold.

14.3 Offering Memo

This is a legal document used to provide potential investors with detailed information about a private offering of securities or real estate. It serves as a comprehensive business plan for investors to evaluate the terms, risks, and potential returns of the investment before making a decision.

14.4 SEC Rule 144A

A provision that modifies the restrictions on the purchase and sale of privately placed securities between qualified institutional buyers without the need for SEC registration.

14.5 Disclosure of Credit Rating Histories

PCR will publish it free of charge in an easily accessible section of its corporate website, the credit rating history as specified in rule 17g7(b) of the Code of Federal Regulations in Excel and in an interactive data file using an XBRL (eXtensible Business Reporting Language) format, and it must be updated at least monthly.

15. Submission of information to the SEC

PCR will submit to the SEC the information contained in **Exhibit 7, "Schedule of Regulatory Filings with the SEC." Regulatory Information to the SEC."**

The annual information required by SEC rules shall include a statement signed by the person responsible for reporting. The annual information required by rule (17g3-a7) shall include a statement signed by the chief executive officer.

Reports must be filed or sent to the SEC, as applicable, electronically via the EDGAR System.

ANNEX 1. AFFIDAVIT FOR PCR DIRECTORS, OFFICERS, AND EMPLOYEES

_____to the ____of _____of _____
(Country and City) (Day) (Month) (Year)

I _____with Unique Identification Document or passport _____, hereby declare that I have been provided with the Conflict of Interest Policy for my review and compliance, as well as the internal manuals governing PCR, which I have read and understood the principles, provisions, and obligations contained in said documents. I further confirm my commitment and adherence to these and declare that during and for the duration of my stay with the company, I will comply with them.

Likewise, I undertake to immediately report any situation that could generate a conflict of interest on my part or on the part of my co-workers, immediate boss, and superiors.

Sincerely,

Employee Signature: _____

Instructions:

(i) This form must be submitted by any employee who is aware of a situation, whether their own or someone else's, that could give rise to a potential conflict of interest in terms of the provisions of the Conflict of Interest Policy.

(ii) In general terms, all situations, usually of a financial or personal nature, that could be presumed to influence an individual's judgment and prevent them from making decisions in an objective, honest, and independent manner must be reported.

ANNEX 2. PERSONAL CONFLICT OF INTEREST FORM PCR

⚠ **Importante:** Esta información es requerida por el área de Cumplimiento. Debe actualizarse anualmente o cuando se realice una modificación a la misma.

INFORMACIÓN POLÍTICA

¿Es militante en algún partido político?

○ Sí ◉ No

RELACIONES CON TERCEROS

Relación con terceros dentro de PCR

○ Familiar en primer grado ○ Familiar segundo grado ◉ Ninguna relación ○ Otro

PARIENTES EN PUESTOS GERENCIALES

¿Pariente con algún puesto gerencial en algún cliente de PCR?

○ Sí ◉ No

ANTECEDENTES PENALES

¿Ha sido sujeto a un proceso penal por delito grave?

○ Sí ◉ No

AHORROS, DEPÓSITOS, INVERSIONES EN EL SISTEMA FINANCIERO (PROPIOS)

Nombre de la Entidad Financiera	Tipo de cuenta, depósito o instrumento financiero	Acciones
Ej: Banco de Crédito	Ej: Cuenta de ahorros	✖

+ Agregar Entidad Financiera

AHORROS, DEPÓSITOS, INVERSIONES EN EL SISTEMA FINANCIERO DE MI CÓNYUGE, CONCUBINA, PADRES, HERMANOS E HIJOS

Nombre de la Entidad Financiera	Tipo de cuenta, depósito o instrumento financiero	Parentesco	Acciones
Ej: Banco Continental	Ej: Depósito a plazo fijo	Ej: Esposa	✖

+ Agregar Entidad Financiera Familiar

APPENDIX 3. TABLE OF SANCTIONS

Types of Policy Violations:

- Conflicts of Interest
- Independence
- To prevent misuse of non-public or confidential information
- Any other PCR policy

Criteria for the severity of the violation

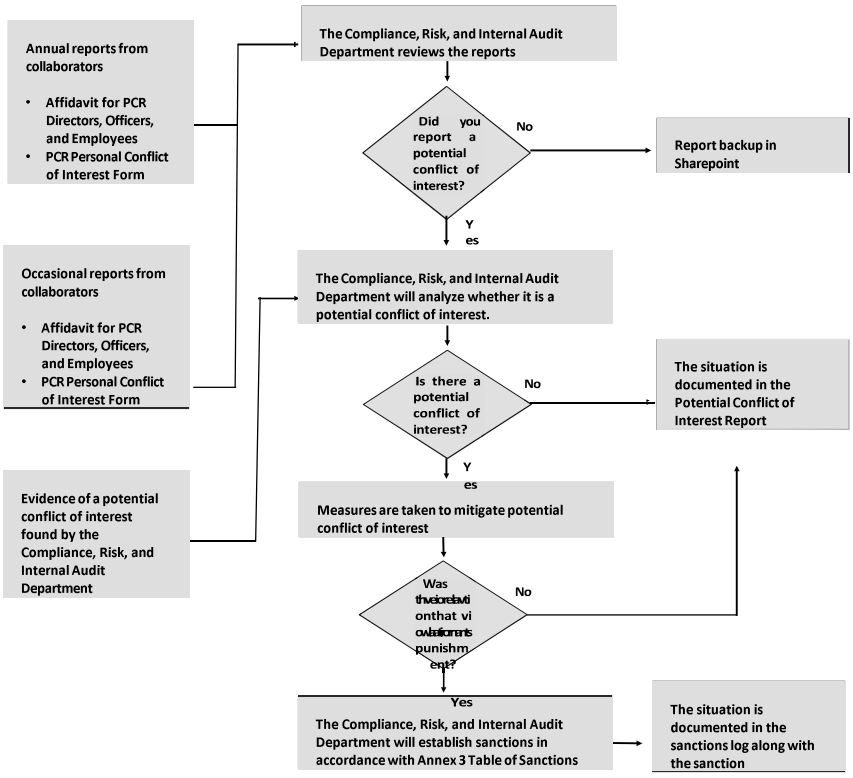
- First offense without consequences – Minor
- Repeat offense – Moderate
- Concealment of non-compliance – Serious
- Sexual harassment – Serious
- Caused impact – Very serious
- Damaged the institution's image – Very serious
- There was intent – Very serious

The penalty will depend on the severity of the offense

- Minor – Verbal warning
- Moderate – Written warning
- Serious or very serious – Suspension or dismissal

The breach and its consequences will be classified according to the regulations of each country.

ANNEX 4. PROCEDURE FOR HANDLING POTENTIAL CONFLICTS OF INTEREST



ANNEX 5. LIST OF DOCUMENTS TO BE RETAINED

The list of documents that must be retained and their minimum retention period are defined below.

(a) 240.17g2 (SEC rule) Records that must be kept and retained by the rating agency	Document	Retention period
(1) Original records in the rating agency's accounting system and records reflecting entries and balances in all accounts in the rating agency's general ledger for each fiscal year.	• External auditexternal of financial statements • Accounting records	5 years
(2) Records regarding each current credit rating from the rating agency (as applicable).	• Electronic electronic of the client • PCR Yes • Minutes of the Committee Risk Rating • Rating report and/or press release	5 years
(3) An accounting record of each person (e.g., a debtor, issuer, subscriber, or other user) who has paid the rating agency for the issuance or maintenance of a credit rating.	• Service agreement • Electronic electronic Client • SFI	5 years
(4) A record of each subscriber's account for the rating agency's credit rating and/or credit analysis reports, indicating the subscriber's identity and address.	N/A (PCR has no subscribers)	N/A
(5) A register listing the general types of services and products offered by the rating agency	• PCR page in the "Services" tab	5 years
(6) A record documenting the procedures established and methodologies used by the rating agency to determine credit ratings.	• Manuals, guides, and policies of the rating agency • PCR methodologies	5 years
(7) A record listing each security and money market instrument and its corresponding credit rating issued by an asset pool or as part of any asset-backed securities transaction in which the rating agency, in determining the credit rating of the security or money market instrument, treats the assets within such pool or as part of such transaction that are not subject to a credit rating by the rating agency.	N/A (PCR does not have asset-backed securities authorized as NRSRO)	N/A
(8) For each outstanding credit rating, a record showing all rating actions and the date of such actions from the initial credit rating to the current credit rating, identified by the name of the rated security or obligor and, if applicable, the CUSIP of the rated security or the Central Index Key (CIK) number of the rated obligor.	• Electronic file electronic Client • Minutes of the Committee Risk Rating • Rating report and/or press release • PCR Yes	5 years
(9) A record documenting the policies and procedures that the rating agency must establish, maintain, and enforce in accordance with the section	• Conflict of Interest Policy	5 years and another 5 years after the date of date of

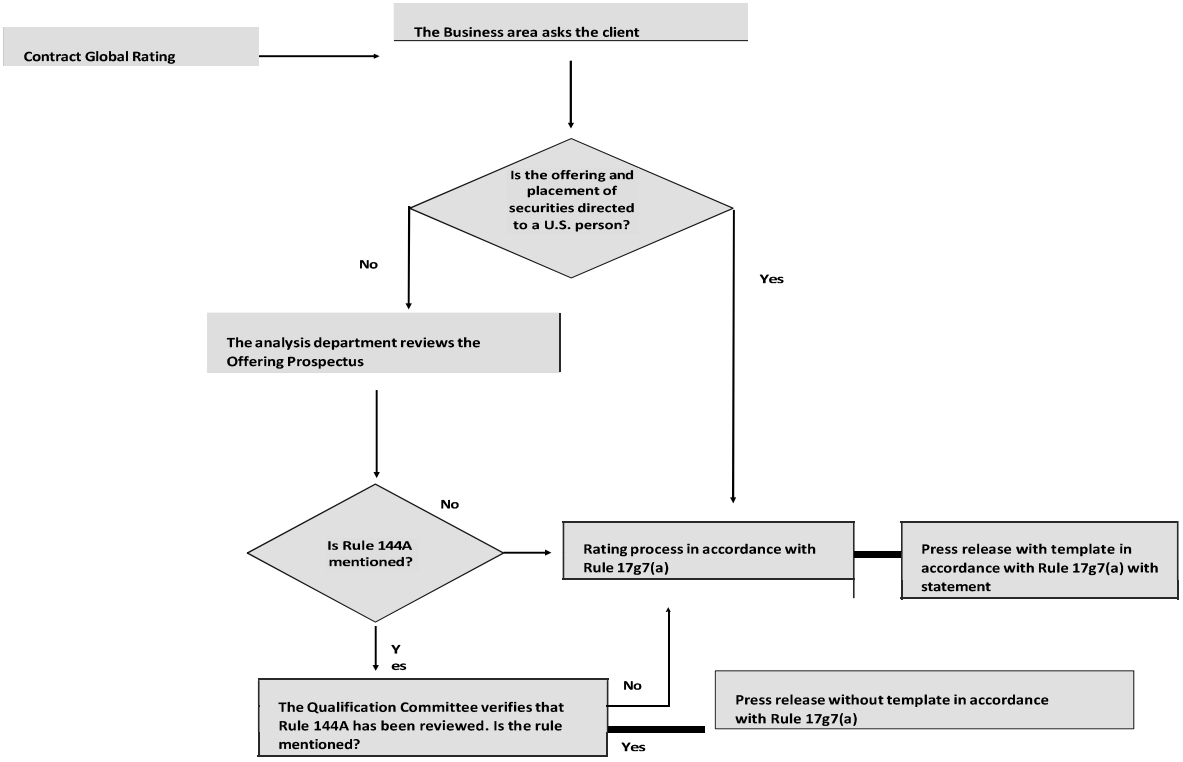
(a) 240.17g2 (SEC rule) Records that the rating agency must make and keep	Document	Retention period
15E(h)(4)(A) of the Act (15 U.S.C. 78o-7(h)(4)(A)) and § 240.17g-8(c). **Look back review**.		Record by another updated

(b) 240.17g2 (SEC Rule) Records to be retained by the rating agency	Document	Retention period
(1) Significant records (e.g., bank statements, invoices, and trial balances) on which the information included in the annual financial reports that the rating agency submitted to or provided to the Commission, as applicable, pursuant to section 240.17g-3 is based.	• Supporting documents for financial statements • Accounting records	5 years
(2) Internal records, including non-public information and working papers, used to form the basis of a credit rating issued by the rating agency.	• Preliminary report • Working drafts	5 years
(3) Credit analysis reports, credit assessment reports, and private credit rating reports from the rating agency and internal records, including non-public information and working papers, used to form the basis of the opinions expressed in these reports.	• Client electronic file • Minutes of the Committee Risk Rating • Rating report or press release • PCR Yes	5 years
(4) Compliance reports and compliance exception reports.	• Compliance reports • Audit reports • Risk reports • Ethics and Conduct Policy • No exceptions	5 years
(5) Internal audit plans, internal audit reports, documents relating to follow-up measures on internal audits, and all records that the rating agency's internal auditors deem necessary to perform the audit of an activity related to its activity as a credit rating agency.	• Annual Annual audit program, • Risk program • Annual of internal audit	5 years
(6) Advertising material of the rating agency that is published or made available to persons not associated with the rating agency. rating agency.	• PCR page • LinkedIn	5 years
(7) External and internal communications, including electronic communications, received and sent by the rating agency and its employees, related to the initiation, determination, maintenance, monitoring, modification, or withdrawal of a credit rating.	• Employee emails • PCR Yes • Client folder • Analysis documents	5 years
(8) Any written communication received from persons not associated with the rating agency containing complaints about the actions of a credit analyst in initiating, determining, maintaining, monitoring, modifying, or withdrawing a credit rating.	Complaints file	5 years

(b) 240.17g2 (SEC Rule) Records to be retained by the rating agency	Document	Retention period
(9) Internal documents containing information, analysis, or statistics used to develop a procedure or methodology for treating another rating agency's credit ratings in order to determine a credit rating for a security or money market instrument issued by an asset pool or part of any transaction asset-backed securities transaction.	N/A (PCR does not have asset-backed securities authorized as NRSRO)	N/A
(10) For each security or money market instrument identified in the record to be prepared and maintained under subsection (a)(7) of this section, any document containing a description of how assets within that pool or as part of that transaction that are not rated by the rating agency but are rated by another rating agency were treated for purposes of determining the credit rating of the security or money market instrument.	N/A (PCR does not have asset-backed securities authorized as NRSROs)	N/A
(11) NRSRO forms (including attachments and accompanying information and documents) to the rating agency submitted or provided, as applicable, to the Commission.	• Intranet, Compliance Compliance • PCR page	5 years
(12) The internal control structure that the rating agency is required to establish, maintain, enforce, and document in accordance with section 15E(c)(3)(A) of the Act (15 U.S.C. 78o-7(c)(3)(A)). **Internal control structure**	• Ethics and Conduct Policy • Conflict of Interest Policy	5 years and another 5 years after the date of replacement registration by another updated one
(13) The policies and procedures that the rating agency must establish, maintain, enforce, and document in accordance with § 240.17g-8(a). **Policies for the rating process and management and approval of methodologies**	• Manual Operating Risk Rating • Conflict of Interest Policy	5 years and another 5 years after the date of replacement of the record with another updated
(14) The policies and procedures that the nationally recognized statistical rating organization must establish, maintain, enforce, and document in accordance with § 240.17g-8(b). **Define Rating Scales**	• Manual Operational Risk Rating • Risk Rating Categories	5 years and others 5 years after the date of replacement of the record with another updated
(15) The standards for training, experience, and competence of credit analysts that the rating agency must establish, maintain, enforce, and document in accordance with § 240.17g-9. **Training and experience of analysts**	• Annual training plan • MOF • Exhibit 8	5 years and another 5 years after the date of replacement of the record with an updated one updated

One original, or a true and complete copy of the original, of each record that must be retained in accordance with paragraphs (a) and (b) of this section shall be retained in such a manner that, during the retention period, the Rating Agency's head office and any other office that has performed activities that gave rise to the creation or receipt of the record can easily access the original record or the copy.

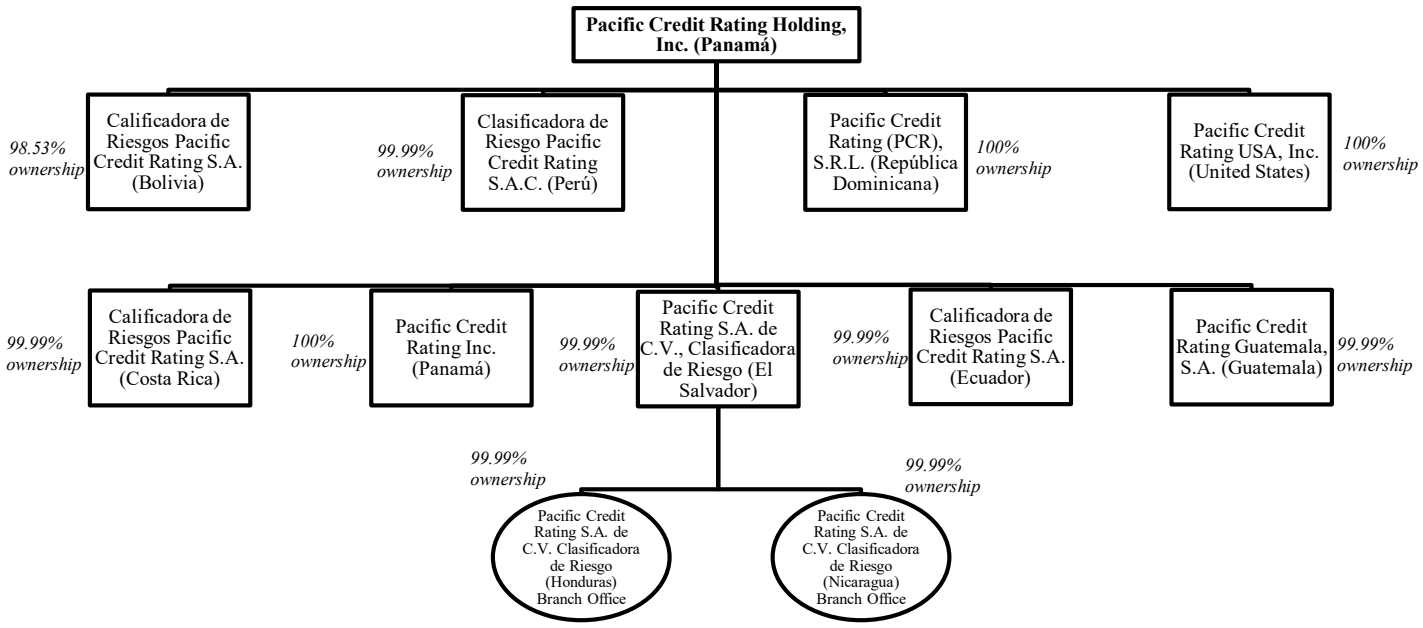
ANNEX 6. PROCEDURE FOR DETERMINING PUBLICATION OF FORM 17g7 (a)(1)



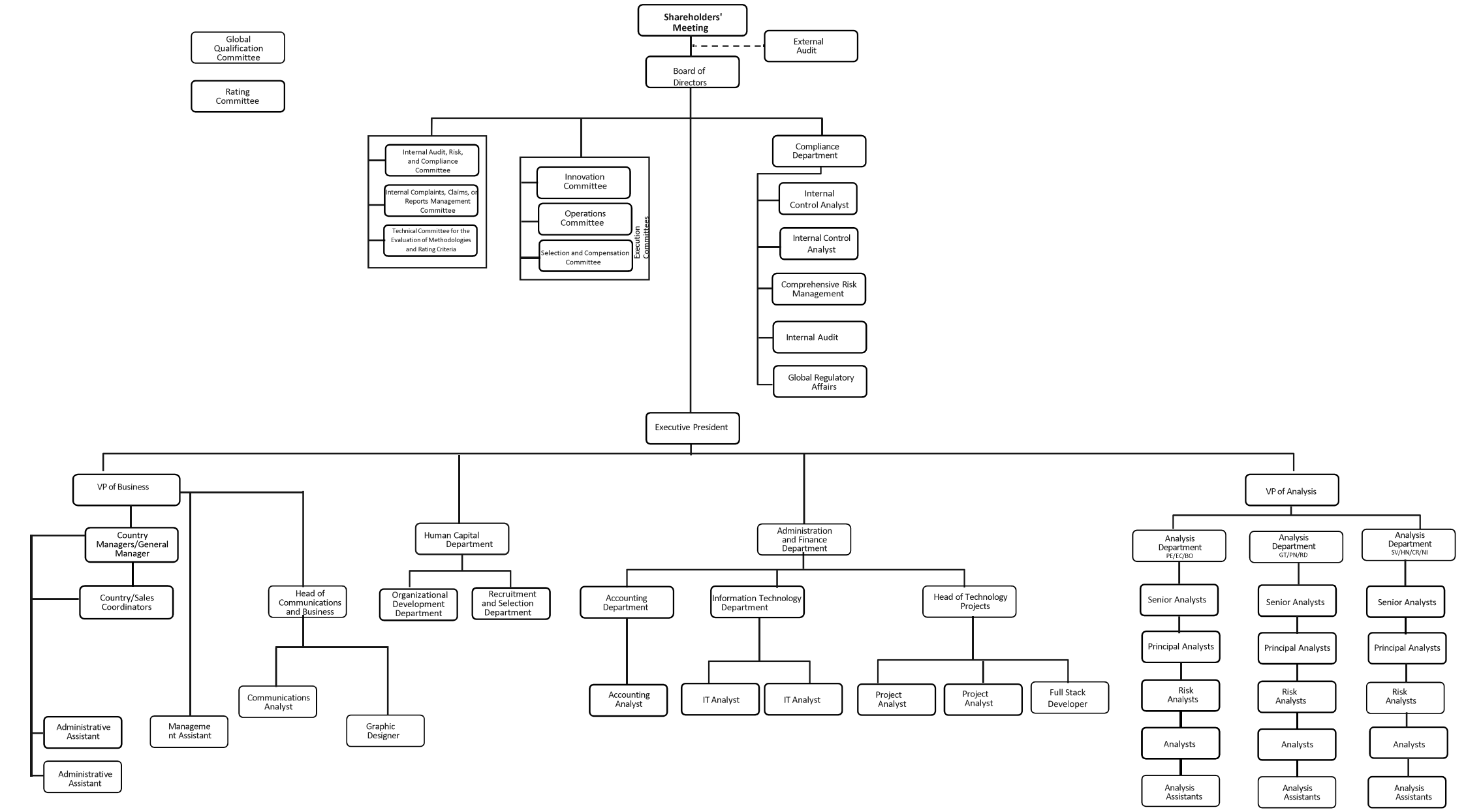
ANNEX 7. SCHEDULE FOR SUBMITTING REGULATORY INFORMATION TO THE SEC

Periodic regulatory information (annual)		Contingent regulatory information	
Deadline: Within the first 90 days natural persons after the end of the calendar year	Significant changes in PCR	**Deadline:** Immediately when substantial in the information previously submitted to the SEC, publication in the up to 10 business days after of its filing with the SEC.	Statistics of measurement of the qualification (Annex
	Statistics of measurement of the rating (Annex		Procedures, scales and
	Procedures, scales and		Policies to prevent the misuse of non-public information (Annex 3)
	Policies to prevent the improper of non-public information (Annex 3)		Organizational structure (Annex 4)
	Organizational structure (Annex 4)		Code of Conduct (Annex 5)
	Code of Conduct (Annex 5)		Policies to avoid conflicts of interest (Annexes 6 and 7)
	Policies to avoid conflicts of interest (Annexes 6 and 7)		Information on analysts (Annex 8)
	Information on analysts (Annex 8)		Information on the compliance officer (Annex 9)
	Information on the compliance officer (Annex 9)		
	Financial report including audited consolidated financial statements (17g3-a1)		
	Financial report including including unaudited consolidated financial statements		
	Information on income (17g3-a3)		
	Analyst compensation (17g3-a4)		
	Top 20 clients (17g3-a5)		
	Rating actions (17g3-a6)		
	Assessment of internal control effectiveness (report of the executive		
	Compliance report (17g3-a8)		

Organization Chart – Subsidiaries and Material Affiliates[1]



[1]All of the affiliates are separate legal entities except Nicaragua and Honduras, whose operation is conducted by the El Salvador entity. Pacific Credit Rating, USA, Inc. is a separate legal entity, wholly owned by Pacific Credit Rating Holding Inc. (Panama). Each credit rating issued by any of the affiliates is on behalf of the NRSRO: Clasificadora de Riesgo Pacific Credit Rating S.A.C. ("PCR"). Each affiliate is subject to the policies and procedures of the applicant, PCR.


Global Qualification Committee
Rating Committee
Shareholders' Meeting
External Audit
Board of Directors
Internal Audit, Risk, and Compliance Committee
Internal Complaints, Claims, or Reports Management Committee
Technical Committee for the Evaluation of Methodologies and Rating Criteria
Innovation Committee
Operations Committee
Selection and Compensation Committee
Execution Committees
Compliance Department
Internal Control Analyst
Internal Control Analyst
Comprehensive Risk Management
Internal Audit
Global Regulatory Affairs
Executive President
VP of Business
Country Managers/General Manager
Country/Sales Coordinators
Administrative Assistant
Administrative Assistant
Management Assistant
Head of Communications and Business
Communications Analyst
Graphic Designer
Human Capital Department
Organizational Development Department
Recruitment and Selection Department
Administration and Finance Department
Accounting Department
Accounting Analyst
Information Technology Department
IT Analyst
IT Analyst
Head of Technology Projects
Project Analyst
Project Analyst
Full Stack Developer
VP of Analysis
Analysis Department PE/EC/BO
Senior Analysts
Principal Analysts
Risk Analysts
Analysts
Analysis Assistants
Analysis Department GT/PN/RD
Senior Analysts
Principal Analysts
Risk Analysts
Analysts
Analysis Assistants
Analysis Department SV/HN/CR/NI
Senior Analysts
Principal Analysts
Risk Analysts
Analysts
Analysis Assistants