Research on Promoting the Adoption of the Global Cross-Border Privacy Rules (GCBPR) System

Research Report

December 1, 2025

Japan Institute for the Promotion of Digital Economy and Community

Table of Contents

I. Outline of the Research

1. Title

Research on Promoting the Adoption of the Global Cross-Border Privacy Rules (GCBPR) System[1] (hereinafter referred to as the "research")

2. Objective

On June 2, 2025, the Global CBPR Forum (hereinafter referred to as the "GCBPR Forum2") officially launched the operation of the GCBPR.

The purpose is to contribute to the effective implementation of public relations and outreach activities to disseminate and raise awareness of the GCBPR, a system that internationally certifies organizations' compliance with certain personal data protection requirements, by conducting research and analysis on the actual state of cross-border personal data transfers.

3. Implementation Details and Framework

3.1. Implementation Details

(1) Project management

Meetings were held monthly in principle to report on progress, etc. (hereinafter referred to as the "monthly progress report"), and necessary materials such as reports, overall schedules, and attachments were sent by three business days prior to the meeting, and as appropriate, the current status was assessed, issues and countermeasures were discussed, and the overall schedule was adjusted.

(2) Research and analysis of the actual state of cross-border personal data transfer

In FY2024, the Ministry of Economy, Trade and Industry (METI) conducted research for promoting the Cross-Border Privacy Rules (CBPR) Certification System (hereinafter referred to as the "2024 Research[3]"). Based on the findings of the 2024 Research, items that should be examined in more detail and those that could not be included in the 2024 Research were the target of study in this research. The following were carried out and the results summarized: 2.1. Questionnaire on Industry-Specific Needs Related to Cross-Border Transfers; 2.2. Interviews with Companies Based on the Questionnaire in 2.1.; 2.3. Detailed Analysis of the Strengths and Benefits of GCBPR; 2.4. Detailed Analysis of the Corporate Certification Process and Study into Improving Its Efficiency.

(3) Recommendations on public relations and outreach activities

Based on the findings of the research in (2), indicators useful in measuring the level of dissemination along with specific recommendations were identified in order to effectively implement public

---

[1] Use “GCBPR” to refer to the system. Where the type of certification is meant, the full names Global CBPR and Global PRP are used.

2 An international system that certifies organizations’ compliance with certain protection requirements for the cross-border transfer of personal data. On April 21, 2022, the declaration of the establishment of the GCBPR Forum—a framework open to participation by countries and regions worldwide—was announced for the purpose of facilitating smoother cross-border transfers of personal data beyond the APEC framework and promoting interoperability among national regulatory systems.

[3] METI website “2024 Research Report” (hereinafter referred to as “2024 Research Report”) https://www.meti.go.jp/policy/external_economy/cbpr/202501.pdf

relations and outreach activities aimed at disseminating GCBPR and increasing the number of participating jurisdictions and business operators.

II. Research and Analysis of the Actual State of Cross-Border Personal Data Transfer

1. Outline of the Implementation

Items that could not be included in the 2024 Research and those that should be examined in more detail were researched and analyzed with the aim of using them in materials for the efficient implementation of public relations and outreach activities to promote the adoption of GCBPR.

2. Findings

2.1. Questionnaire on Industry-Specific Needs Related to Cross-Border Transfers

(1) Objective of the survey

In order to quantitatively research and analyze industry[4]-specific needs related to cross-border transfers (referring to whether or not cross-border transfers are being conducted and concerns regarding such transfers in each industry, and jurisdictions where participation in the system may motivate certification), a questionnaire was conducted using postal mail and online responses for business operators in Japan.

In addition, based on the questionnaire results, business operators were selected as interview targets as described in 2.2. to ask more detailed questions about the questionnaire items, bottlenecks in obtaining GCBPR, and incentives for certification, focusing on industries that were found to have a need for GCBPR certification.

Further, countries and regions in which Japanese business operators have a large number of cross-border personal data transfer transactions were found according to the questionnaire results. After excluding jurisdictions expressing intent to participate in GCBPR, those unlikely to participate, and existing GCBPR members, jurisdictions were selected as indicated in 2.6. Mapping of the Laws and Regulations of Countries and GCBPR Program Requirements for Analysis, for inclusion in the mapping.

(2) Survey period

Thursday, October 2, 2025 to Monday, November 3, 2025

(3) Survey targets

To avoid imbalance in terms of business field and size of business, a total of 2,000 companies, consisting of 100 companies in 20 industries, and about 22,500 companies registered on JIPDEC's direct mailing list, were extracted. The questionnaire was mainly conducted in manufacturing, information and communications, wholesale and retail trade, finance and insurance, and services, which are assumed to be handling a large amount of personal data.

[4] Industry refers to the Division and Major Group classifications in the Japan Standard Industrial Classification (revised October 2013). The same applies hereafter.

Table 1　Breakdown of the 20 industries surveyed

	Japan Standard Industrial Classification		The Japan Standard Industrial Classification
1	Agriculture and forestry, fisheries, mining and quarrying of stone and gravel, construction	11	Information and communications
2	Manufacturing (food, beverages, tobacco and feed)	12	Transport and postal services
3	Manufacturing (textile products, lumber and wood products, furniture and fixtures)	13	Wholesale and retail trade
4	Manufacturing (pulp, paper and paper products, printing and allied industries)	14	Finance and insurance
5	Manufacturing (chemical and allied products, petroleum and coal products)	15	Real estate and goods rental and leasing
6	Manufacturing (plastic products, rubber products, ceramic, stone and clay products)	16	Scientific research, professional and technical services
7	Manufacturing (iron and steel, non-ferrous metals and products)	17	Accommodations, eating and drinking services, living-related and personal services and amusement services
8	Manufacturing (machinery, devices and electronic circuits, electrical machinery, equipment and supplies)	18	Education, learning support
9	Manufacturing (information and communication electronics equipment, transportation equipment)	19	Medical, health care and welfare
10	Electricity, gas, heat supply and water	20	Compound services, services, n.e.c. (not elsewhere classified)

(4)　Number of responding business operators

Valid responses were obtained from 634 companies.

(5)　Survey method

[1]　Postal mail

Questionnaires with URLs and QR codes were mailed to 2,000 target business operators, and responses were collected online.

[2] Email distribution

For the 22,500 registrants in JIPDEC's database, a URL of the questionnaire was distributed by email, and responses were collected online.

(6) Survey questions

The questionnaire was kept at 10 questions to ensure that the response rate did not decrease, and questions were covered basic information regarding the business operators and details related to their cross-border transfers of personal data. The main questions based on this basic information were selected as follows for easy cross-tabulation:

<Cross-border transfers of personal data>

Basic information <attributes>

- Industry: selected from among the 20 industry categories, ranging from agriculture and forestry, fisheries to compound services.
- Number of employees: ten categories, starting with 1-4 up to 10,000 or more
- Net sales: eight categories, from less than 50 million yen to more than 100 billion yen
- Capital: nine categories, from less than 2 million yen to more than 10 billion yen
- Status of third-party certification acquisition for personal information: name of certifications obtained, reasons for not obtaining certification, name of certifications under consideration

Q1: Purpose of the cross-border transfers

Multiple answers were permitted from the following options regarding the purpose of cross-border personal data transfer

- ❑ To provide services pertaining to its own business (including service improvement, new service development, and business streamlining; the same applies hereafter)
- ❑ To manage the company's personnel information
- ❑ To provide services pertaining to joint business between the company and a third party
- ❑ For advertising and marketing of the company's business/joint business with a third party
- ❑ To provide services pertaining to the business of a third party
- ❑ For advertising/marketing of third-party business
- ❑ Other

Q2: Attributes of the transfer destinations

Multiple answers were permitted from the following options for attributes of the recipients

- ❑ Group companies
  (Additional questions if selected) Number of locations, number of employees, and countries/regions
- ❑ Advertising distribution operators (companies whose main business is the distribution of advertisements)
  (Additional questions if selected) Name of the countries/regions
- ❑ Cloud service providers (use of SaaS, etc.)

(Additional questions if selected) Number of services used, details of services, names of operators, and data transfer destinations (countries/regions)

❑ Business operators other than advertising and cloud service providers

(Additional questions if selected) Name of the countries/regions

❑ Government agencies, etc.

(Additional questions if selected) Transfer destinations (countries/regions)

❑ Other

Q3: Type of information to be transferred

With regard to the personal data items being provided, information was divided into employee-related and customer-related, and respondents were asked to select all relevant items along with just one estimated size out of the options provided (units of 10, 100, 1,000, or 10,000) for each type of information.

❑ Employee information
- Name
- Address, phone number, gender, email address
- Facial image
- Individual identification codes, such as biometric information (Article 2, paragraph (2), item (i) of the Act)
- Individual identification codes, such as passport number, driver's license number, and certificate of insured person number (Article 2, paragraph (2), item (ii) of the Act)
- Special care-required personal information (Article 2, paragraph (3) of the Act)
- Location information, activity record, and physical space log data
- Digital space log data, including web-browsing history and online purchases.

❑ Customer information (other than employees)
- Name
- Address, phone number, gender, email address
- Facial image
- Individual identification codes, such as passport number, driver's license number, and certificate of insured person number (Article 2, paragraph (2), item (ii) of the Act)
- Special care-required personal information (Article 2, paragraph (3) of the Act)
- Physical space log data, such as location information, activity record, purchases at physical stores, Digital space log data, including web-browsing history and online purchases.
- Other

Q4: Purpose of use at the transfer destinations

Respondents were asked to select all relevant items regarding the manner of use, etc. by the data recipients.

❑ Contacting individuals and distributing advertisements to them

❑ Managing personnel information

❑ Matching data with other personal information or personal-related information held by the recipient

❑ Analysis and profiling

❑ Compiling statistical information, statistical analysis

❑ Other

❑ Don't know

Q5: Basis for the transfer of personal data

Respondents were asked to select all relevant options regarding the basis for the transfer of personal data.

❑ GDPR: Adequacy decision
❑ GDPR: BCR (Binding Corporate Rules)
❑ GDPR: SCC (Standard Contractual Clauses)
❑ Individual contract concluded
❑ Consent of the individual
❑ The APEC/Global CBPR System
❑ Other

Q6: Consent of the user and use of services

Respondents were asked to choose one of the following results when users do not give consent.

❑ Even if the individual does not give consent to data provision, they may use the services.
❑ If the individual does not give consent to data provision, they may not use the services. (Additional questions if selected)
  - Due to the fact that data provision is indispensable to service provision, services cannot be provided without obtaining consent.
  - Because consent management is difficult/costly
  - Other ( )

Q7: Challenges in cross-border transfers

Respondents were asked to select all relevant items regarding issues they consider challenges in the cross-border transfer of personal data.

❑ It takes time to understand and address the data protection regulations of transfer destinations
❑ Differences in data protection rules between Japan and the transfer destination country make it difficult to coordinate
❑ We are concerned that our current response is not adequate for security control in both legal systems
❑ Costs for concluding contracts and addressing regulations (including legal affairs) are a burden
❑ Cannot receive the same level of rules for handling data as those in Japan (including non-disclosure of necessary information)
❑ Don't know
❑ Do not feel that there are any particular challenges. If you select this response, please explain the reasons. Reasons: ( )
❑ Other

Q8: Countries and regions to which expansion is planned

Respondents were asked to select one response from the following regarding countries and regions to which there are plans to expand as personal data cross-border transfer destinations, or have recently expanded to.

- ❑ Countries and regions to which transfers have recently begun (within the last three years or so)
- ❑ Countries and regions to which cross-border transfers are planned
- ❑ There are no plans to expand beyond the current transfer destinations
- ❑ Downsizing countries and regions as transfer destinations is being planned (specify the reasons)

Efforts regarding the handling of information in general, not limited to cross-border transfers

Respondents were asked regarding the status of efforts concerning the handling of personal information, including those currently taking place or are scheduled to take place in the future.

Q9: Efforts regarding the appropriate handling of personal information

Respondents were asked to answer in free form as to what kind of measures are being taken in the appropriate handling of personal information, such as the establishment of a system to reflect the voices and concerns of customers and public relations activities, providing examples in their response.

Q10: Utilization of information not requiring consent of the individual, etc.

Respondents were asked to select all measures being implemented in utilizing personal information without obtaining the consent of the individual pertaining to use other than for the intended purpose and for provision to a third party.

- ❑ Personal information is processed into statistical information for use
- ❑

Pseudonymously processed personal information is being used

- ❑ Anonymized processed personal information is being used
- ❑ Wide-ranging consent is obtained when acquiring personal information, including for purposes of use that may be needed in the future, and for the act of providing personal data to a third party that may occur in the future
- ❑ No measures are being implemented
- ❑ Other

(7) Questionnaire results

[1] Purpose of the cross-border transfer of personal data (Q1)

Regarding the purpose of the cross-border transfer of personal data, out of 279 companies[5], excluding those that responded they did not have transfer destinations, 180 responded that it was for providing services related to their own business (64.5%), while 130 responded that it was for managing their company's personnel information (46.6%). This indicates that the provision of their own services and personal information management related to their employees are the main purposes of cross-border transfers.

On the other hand, the number of cross-border transfers for advertising/marketing is low, with the number of cross-border transfers "for advertising/marketing of third-party business" (15 companies, 5.4%) being the lowest.

[2] Attributes of the transfer destinations (Q2)

Of the 257 companies excluding those that responded that they do not have transfer destinations, a high percentage chose "cloud service providers (use of SaaS, etc.)" (87 companies, 33.9%) and "group companies" (82 companies, 31.9%). Details are as follows.

Table 2 Attributes of the transfer destinations

Attributes of the transfer destinations	Key details by attribute
Cloud service providers (87)	- While more than 80% of companies use the cloud services of no more than five providers (72 companies, 82.8%), a small number of companies use the cloud services of 21 or more providers (4 companies, 4.6%). Response for the number of countries as data transfer destinations was greatest for one country (55 companies, 63.2%), followed by two countries (16 companies, 18.4%). - The most commonly used services were business management and infrastructure services, such as storage and groupware, communication, attendance management, and disaster safety confirmation. <Most-used services>*% shows the percentage of the 87 companies • Microsoft 365 (Teams, Outlook, OneDrive, etc.): Approx. 60% • Google Workspace (Gmail, Drive, Meet, etc.): Approx. 40% • AWS (Amazon Web Services): Approx. 25% • Zoom: Approx. 20% • Slack, Box, Salesforce: Approx. 15% each

[5] The total number of companies for Q1 is 634; however, after excluding 355 companies that selected “Other” and indicated that they do not have transfer destinations, the base number derived is 279 companies. To ensure the accuracy of responses, the number of companies for Q2 to Q7 differs from question to question because those that indicated they do not have transfer destinations were excluded from the calculation in determining the base number.

Attributes of the transfer destinations	Key details by attribute
Group companies (82)	- The response for the number of overseas subsidiary locations was greatest for five or fewer (56 companies, 68.3%), followed by 51 or more (10 companies, 12.2%). For the number of employees, there was no difference among the various options, except that 40% of respondents had 101 or more employees (34 companies, 41.5%). - As for the countries and regions in which they are located, the response was greatest for one country (41 companies, 50%), followed by five countries (15 companies, 18.3%). As with the number of locations, the responses were largely divided into two categories, i.e. large and small numbers.

[3] Type of information to be transferred (Q3)

Of the 284 companies excluding those that responded that they did not have transfer destinations, 194, or 68.31% of the total, chose employee information, while 137, or 48.24%, chose customer information (other than employees) as the type of personal data to be transferred. Among the 194 companies that chose employee information, the main information items were name (191 companies, 98.5%), and address, phone number, gender, and email address (164 companies, 84.5%). Similarly, the percentages for these two items were also high for customer information.

[4] Purpose of use at the transfer destinations (Q4)

Of the 338 companies, excluding those that did not have transfer destinations, the largest number of cases were related to the management of personnel information. (126 companies, 37.3%), followed by contacting the individuals and distributing advertisements (93 companies, 27.5%).

[5] Basis for the transfer of personal data (Q5)

Of the 272 companies, excluding those that responded that they do not have transfer destinations, the most common basis for the transfer of personal data was the consent of the individual (202 companies, 74.3%), followed by individual contract concluded (119 companies, 43.8%).

On the other hand, few companies responded that "GDPR: Adequacy decision" (68 companies, 25.0%) and "GDPR including BCR and SCC" were the basis for transfer. Many respondents who answered "Other" chose "No" but a considerable number of respondents answered "Don't know."

[6] User consent and service usage (Q6)

Approximately 70% of business operators said individuals are not able to use the services (454, 71.6%) when they do not give consent.

Of the 253 companies, excluding those that responded they do not have transfer destinations, more than 90% cited "Due to the fact that data provision is indispensable to service provision, services cannot be provided without obtaining consent" (236 companies, 93.3%). It became evident that without data provision, practically no services can be provided for use.

[7] Challenges in cross-border transfers (Q7)

Of the 524 companies excluding those that responded that they do not have transfer destinations, the top responses were "It takes time to understand and address the data protection regulations of transfer destinations" (195 companies, 37.2%), and "Differences in data protection rules between Japan and the transfer destination country make it difficult to coordinate" (166 companies, 31.7%).

Many respondents also chose "Don't know" (174 companies, 33.2%).

[8] Countries and regions to which expansion is planned (Q8)

With regard to future expansion of cross-border transfer destinations, many business operators have shown a tendency to maintain the status quo. It was also found that the countries and regions where expansion of cross-border transfers is planned by business operators are the United States, Europe, Southeast Asia, the Middle East, and Africa, with various countries and regions being considered and no bias toward a specific region.

A small number of business operators responded that they were planning to reduce the number of cross-border transfer destinations, and the reasons for the reduction included cost savings and mitigating country risk.

[9] Efforts regarding the appropriate handling of personal information (Q9)

It was found that many business operators have, as efforts toward the appropriate handling of personal information, established contact points to gather the opinions of customers specific to the handling of personal information, and introduced measures regarding the use of personal data on their own websites. Many businesses with the PrivacyMark[6] have established systems in compliance with JIS Q 15001 and conducted periodic internal audits and training pursuant to the establishment and operation guidelines.

[10] Utilization of information not requiring consent of the individual, etc. (Q10)

Regarding measures for the utilization of personal information not requiring consent of the individual, the greatest percentage of companies responded that no measures are being implemented (436 companies, 69.5%).

Those that reported implementing such measures most commonly indicated that they specify broad purposes of use when acquiring personal information, including for purposes of use that may be needed in the future and for the act of providing personal data to a third party that may occur in the future (98 companies, 15.6%), followed by the use of personal information for statistical purposes (61 companies, 9.7%).

(8) Summary of questionnaire results

According to this research, the transfer of personal data at Japanese companies to cloud service providers and group companies was mainly for the purpose of providing their own services and managing personnel information. The basis for transfers was mainly consent of the individual.

Meanwhile, it became clear that the main issues in cross-border transfers are that it takes time to understand and address the data protection regulations in various countries, and that it is difficult

[6] A mark that signifies trust, that can be used by registered operators (companies and organizations) that have been assessed as having set up a system for appropriately handling personal information.

to make adjustments for differences in data protection rules between Japan and the transfer destinations.

2.2. Interviews with Companies Based on the Questionnaire in 2.1.

(1) Research objective

To obtain detailed responses to the questionnaire items and conduct interviews regarding bottlenecks in GCBPR certification for companies in industries that were found to have a need of GCBPR based on the questionnaire in 2.1., and summarize issues related to third-party certification systems, including GCBPR.

(2) Interview period

Tuesday, November 11, 2025 to Thursday, November 27, 2025

(3) Research targets

Among the business operators that agreed in the questionnaire in 2.1. to take part in an interview, we examined the industry, business field, and size of the business, then conducted interviews with a total of nine companies, including one company already GCBPR certified (hereinafter referred to as a "certified organization").

The interviews were conducted with business operators (including Japanese certified organizations) who could adjust their schedules to accommodate the interview period of this research. Business operators that do not have cross-border transfers of personal data and those that mistakenly responded that they have the capability to manage such transfers were excluded.

A summary of the interview target business operators is as follows.

Table 3 Record of the survey interviews

	Date and time	Target business operators
1	Tuesday, November 11, 2025 13:00-14:00	Company A (Compound services, services, n.e.c.) <Event/experiential marketing>
2	Wednesday, November 12, 2025 13:30-14:30	Company B (Information and communications) <System development and maintenance>
3	Friday, November 14, 2025 14:00-15:00	Company C (Compound services, services, n.e.c.) <IT and human resource services>
4	Thursday, November 20, 2025 10:00-11:00	Company D (Information and communications) <Electronic payment services>
5	Friday, November 21, 2025 10:30-11:30	Company E (Information and communications) <Software development, etc.>
6	Tuesday, November 25, 2025 10:00-11:00	Company F (Information and communications) <Consulting>
7	Tuesday, November 25, 2025 16:00-17:00	Company G (Education, learning support)
8	Wednesday, November 26, 2025 10:00-11:00	Company H (Scientific research, professional and technical services)
9	Thursday, November 27, 2025 10:00-11:00	Company I (Compound services, services, n.e.c.) <System sales and maintenance>

Table 4　Attributes of interview target business operators

Industry	Number of employees	Net sales
Information and communications	20 - 49	100 million to less than 1 billion yen
Information and communications	100 - 299	1 billion to less than 5 billion yen
Information and communications	1,000 - 4,999	10 billion to less than 50 billion yen
Information and communications	5,000 - 9,999	100 billion yen or more
Compound services, services, n.e.c. (not elsewhere classified)	50 - 99	1 billion to less than 5 billion yen
Compound services, services, n.e.c. (not elsewhere classified)	50 - 99	5 billion to less than 10 billion yen
Compound services, services, n.e.c. (not elsewhere classified)	500 - 999	10 billion to less than 50 billion yen
Education, learning support	1,000 - 4,999	5 billion to less than 10 billion yen
Scientific research, professional and technical services	50 - 99	1 billion to less than 5 billion yen

(4)　Survey items

The interview consisted of 16 question items (a total of 27 questions), including the type of business operations that may result in the cross-border transfer of personal data, the countries and regions of the cross-border transfer destinations and the contracted parties, whether there are any problems related to agreements with the contracted parties, awareness level of GCBPR, incentives for certification, and the state of certification systems obtained other than GCBPR, as well as the dissemination and spread of GCBPR in Japan.

Specific interview question items are as follows.

Table 5　Interview question items

Question description
1. Which of the following do operations involving cross-border transfer of personal data fall under? [1] Outsourcing (with more than one transfer destination or contracted party) [2] Only exchanging employee information with overseas subsidiaries (limited transfer destinations)

Question description
2. Please tell us about the status of cross-border transfers of personal data and how personal data are being handled at the transfer destinations. [1] How many countries or regions do you transfer the personal data to? [2] Also, please tell us if you have any problems related to contracts with transfer destinations. For example, understanding the legal system of transfer destinations and costs incidental thereto, labor required in preparing the contract [3] Roughly how many contracted parties do you have for personal data? e.g., status of outsourcing operations using cloud services (SaaS, etc.)
3. Have you ever heard about Global CBPR certification[7] or the APEC CBPR certification? (Level of understanding: have heard of them, looked into, considered certification, etc.)
4. Do you know that the names of CBPR-certified organizations are published on the websites of the competent authorities for the CBPR certification system (the Personal Information Protection Commission and the Ministry of Economy, Trade and Industry) as well as the assessment body (JIPDEC), etc.?
5. What is the reason your company has not obtained Global CBPR or APEC CBPR certification?
6. What is the most important determining factor if considering certification?
7. If you were to consider CBPR certification (and also if you are already in the consideration process), what information, in addition to a general explanation of the CBPR certification system, provided by websites of the competent authorities (the Personal Information Protection Commission and the Ministry of Economy, Trade and Industry) and the assessment body (JIPDEC), would facilitate consideration? e.g., specific cost estimates, time required for certification, information on certified organizations in Japan and other countries, and opinions from already certified organizations as to the specific benefits gained by being certified
8. Can the following be incentives for certification? • Names of business operators being published on the websites of competent authorities and the assessment body as noted in Q4 • An ecosystem (network) being created for the appropriate handling of cross-border data between certified organizations, competent authorities, the assessment body, etc. through CBPR
9. Are there any other companies in the same industry or business partners (including overseas business operators) that have obtained the Global CBPR/APEC CBPR certification?
10. Do you think that Global CBPR certification is effective (needed) for business operators? Response: Yes/No Reasons:
11. What are the benefits and drawbacks of Global CBPR certification /APEC CBPR certification when compared with GDPR and other regulations and laws (e.g., adequacy decision/BCR/SCC)?

[7] In the main text of the report, the term "GCBPR" is used to describe the certification system, but for the interview question items, the wording was changed to "GCBPR certification" to make it easier to understand for the business operators being interviewed.

Question description
12. Have you obtained any certifications excluding CBPR? ➢ We have [1] Name of certification systems [2] Reasons for obtaining certification [3] Effects of the certification systems [4] Are there any parts of the application procedures and operations after certification where you would like improvements to be made? ➢ We have not. [1] Reasons: [2] Scheduled upcoming certifications - Yes: Name of the certification systems to be obtained - None: Reasons
13. What do you most expect from third-party certification systems, including CBPR certification and others?
14. This is regarding GCBPR group certification, which is not available in Japan. * Group certification refers to certification that covers subsidiaries, on the assumption that they handle information under the same privacy policy as the parent company. Currently in Japan, certification is obtained on a company-by-company basis, while in the U.S. and Singapore, group certification is possible. ➢ Japanese subsidiaries: If you have domestic subsidiaries, does the operation of the certification system to include subsidiaries being certified together with the parent company (assuming that they thoroughly enforce the same policy as the parent company) lead to motivation in obtaining CBPR certification? ➢ Overseas subsidiaries: If you have overseas subsidiaries, does the operation of the certification system to include subsidiaries being certified together with the parent company (assuming they thoroughly enforce the same policy as the parent company) lead to motivation in obtaining CBPR certification? ➢ Do you think it would be better to have group certification, regardless of whether you have subsidiaries? Response: Yes/No Reasons:
15. This is regarding GCBPR PRP certification, which is not available in Japan. * PRP certification is for processors (vendors, cloud service providers, and other businesses that process customer data that they receive from clients). Japan does not recognize a legal distinction between controllers and processors, with both in the same category of "personal information handling business operator." ➢ Will you be motivated to obtain CBPR certification if PRP certification is initiated? ➢ Do you think it would be better to have PRP certification, regardless of whether you are a processor or not? Response: Yes/No Reasons:

Question description
16. This question involves the expansion of Global CBPR certification in Japan. ➢ What methods do you think are effective in raising awareness? ➢ As a measure during the expansion stage, do you think that benefits such as free review fees for a certain period are effective in growing the number of certified organizations? ➢ What do you think needs to be done to make cross-border transfer tools, such as CBPR certification, more appealing to business operators in Japan? e.g., publicize its effectiveness as a tool in demonstrating compliance or accountability, give it influence over contract acquisition (e.g., for new contracts, government-commissioned projects, etc.)

(5) Interview method

Interviews were conducted as online meetings. After the Personal Information Protection Commission explained the purpose of the interview, the organization in charge conducted interviews with the business operators and further confirmed details related to the responses as necessary.

(6) Interview results[8]

Q1. Which of the following do operations involving cross-border transfer of personal data fall under?

[1] Outsourcing (with more than one transfer destination or contracted party)

[Overview]

Six out of nine business operators responded that they fall under [1]. These business operators carry out cross-border transfers of personal data through outsourcing operations to overseas development bases and by using cloud services (SaaS). While the United States was the main transfer destination, some business operators transferred data to several countries and regions, including India, Europe, the Middle East, and Southeast Asia. Business operators that handle user information on a large scale were found to transfer user and employee information for development operations at overseas locations. In addition, business operators conducting overseas surveys as part of think tank operations are characterized as having outsourced vendors for interviews and surveys in multiple countries.

It was also confirmed that business operators engaged in work for public entities are using cloud services related to GIS (Geographic Information Systems) and cross-border transfers are occurring because servers are located abroad. Business operators engaged in translation and interpretation services use several SaaS, such as translation support tools and online meeting tools, and there have been cases where there are more than 40 contracted parties.

<Key opinions from respondents>

- From the perspective of cross-border transfers, we handle personal data when using overseas cloud services such as Box and OneDrive, for example.
- We do exchange employee information with overseas subsidiaries, but outsourcing is the main business.

[8] Q1 - Q16 are interview question items common to all business operators, and four additional questions are separately asked to certified organizations.

[2] Only exchanging employee information with overseas subsidiaries (limited transfer destinations)

[Overview]

Three out of nine business operators responded that they fall under [2]. In all cases, the parent company or business partners were situated overseas, and only specific information such as employee information and student information was exchanged on a limited basis. The transfer destination is limited to one country, either the United States or the EU region, and the scope of transfer is narrower than that of the outsourcing. However, if the parent company is located overseas, it is necessary to comply with the rules and systems of headquarters, and it was shown that compliance with the local legal system is an issue.

<Key opinions from respondents>

- We collaborate with universities overseas and provide Japanese student information to them. Although outsourcing or overseas subsidiaries are not involved, personal data are being transferred overseas. We have concluded an agreement through a law firm that includes jurisdictions overseas and are looking to expand into the Asian region in the future.
- Our overseas subsidiary is located in the Asian region and we exchange employee information.

[3] Other (examples that do not clearly correspond to either)

For some business operators, neither [1] nor [2] were clearly applicable. Specifically, these business operators do not outsource or have overseas subsidiaries, but through the use of cloud services (file sharing services, business card management services, etc.), they may be unintentionally transferring personal data overseas. These business operators had poor awareness that they were engaged in cross-border transfers, and they were unable to accurately identify countries and regions as transfer destinations.

Q2. Please tell us about the status of cross-border transfers of personal data and how personal data are being handled at the transfer destinations.

[1] How many countries or regions do you transfer the personal data to?

[Overview]

The number of countries and regions that are transfer destinations varied greatly depending on the type and scale of business operators. The most common pattern was the transfer to the United States associated with the use of cloud services. Almost all business operators fell under this pattern. On the other hand, there were transfers to multiple countries and regions, such as Asia, the Middle East, and Europe, among business operators with development bases and subsidiaries overseas, as well as business operators engaged in overseas research operations. In addition, it became evident that many business operators using cloud services are aware of the location of the service provider's headquarters, but do not have an accurate understanding of where the actual server is located.

There were also some instances where cloud service providers were not disclosing the specific location of their servers even when inquired. Some business operators were concerned that their information was further spreading, even if they were told that the safety of information was secured with a distributed backup system.

<Key opinions from respondents>

- Our headquarters are in the United States, and we use a common personnel management system. I know the headquarters location, but not where the system servers are located.
- Based on the location of the headquarters of the cloud service providers we are using, the United States, Switzerland, and Germany are the main transfer destinations.
- We use cloud services (file sharing services, etc.), but it is not clear where the services of service providers are being carried out, and transfer destination countries have not been identified.

[2] Are there any problems related to contracts with transfer destinations?

[Overview]

Only a few respondents said that they do encounter problems at the contract conclusion stage. However, it became clear that many business operators that undergo cross-border transfers share many of the same problems, such as insufficient understanding of the legal systems in the transfer destination countries, difficulty obtaining information on legal amendments, disparities in bargaining power with cloud service providers, and uncertainty in data handling upon termination of service use.

Specifically, regarding contracts based on terms of use, which is common with SaaS usage, difficulty determining the extent to which the terms of use should be reviewed; difficulty finding contact information for overseas business operators; and the materials provided being in a non-Japanese language were pointed out. Consequently, collecting information requires substantial time. For business operators with the parent company or business partners located overseas in particular, handling compliance with the local legal system concerning the protection of personal information was an issue. Small and medium-sized companies (SMEs) also expressed concern that it might be difficult for their own requirements to be met in contracts with major cloud service providers.

<Key opinions from respondents>

- It is necessary to comply with both local laws governing overseas parent companies and Japan's Act on the Protection of Personal Information, and information not being provided to us when local laws are revised is an issue. The handling of information stated in the contract at the start of employment is based on foreign laws and is difficult for the person in charge of employment contracts to explain.
- We have hired a law firm with offices both in Japan and overseas to handle matters, and while there are no contractual issues at this time, it was difficult finding experts.
- Currently, there are no major problems since our use is mainly cloud services. However, if customers raise any issues regarding the use of services overseas in the future, we may need to engage in close communication with major service providers. In that case, there is concern over the extent to which requests from small business operators such as ours would be accommodated. At the stage of selecting and evaluating providers for cloud service use, a key issue is determining the extent to which we should investigate information that is not publicly disclosed. In particular, it is not stated how entrusted personal information will be handled once the service ends, and it is unclear how to respond if we are faced with a sudden notice of termination.

[3] Roughly how many contracted parties do you have for personal data?

[Overview]

Although the number of contracted parties varies by business operator, many operators use cloud services (SaaS), and they effectively become the contracted parties. Specific responses included file-sharing and storage services, personnel management systems, business card management systems, and cloud infrastructure (AWS, Google Cloud, etc.). The number of contracted parties ranged from two to three, to more than 40. In business operations that use a large number of SaaS, such as for translation/interpreting services, in some cases the number of contracted parties was as much as 25 counting only cloud service providers, and including other contracted parties, totaled more than 40.

On the other hand, some business operators did not recognize the use of cloud services as entrustment, and the differences in perceptions of cross-border transfers became apparent. There were also some business operators that have a policy in place to use domestic servers as much as possible, but some functions have not been able to completely eliminate the possibility of overseas servers being used.

<Key opinions from respondents>

[Less than 10 companies]

- There are only two services that share files with headquarters. The file-sharing service was not recognized as a contracted party, but it is applicable in the sense that they manage the information.
- We do not entrust information. Online conference tools, etc. are only used domestically, and no cross-border transfers are taking place.
- We use a total of three companies: two file sharing services and one business card management service. I do not know whether the business card management service has servers overseas.

[Between 10 and 30 companies]

- Cloud services being used are from roughly 10 companies, including major IT business operators, cloud storage, online conferencing tools, remote access tools, and cloud infrastructure.

[More than 30 companies]

- There are 25 cloud service providers and 18 other companies (e.g., outsourcing to parent company, rental servers, and delivery companies).

Q3. Have you ever heard about Global CBPR certification or the APEC CBPR certification?

[Overview]

Awareness was found to be generally low, and level of recognition was broadly classified into three categories.

First, had no recognition at all and heard about them for the first time.

Second, had only a superficial awareness of them, having heard the names before.

Third, had obtained information on them through seminars, etc.

The second pattern was the most common, with many business operators who had seen the names in newsletters and information emails from the assessment body and their website, but did not know details of the systems. In particular, some business operators that use SaaS were aware that CBPR is something SaaS providers should obtain, but had not yet recognized the notion that they themselves are in a position that requires certification.

Additionally, in almost all cases, business operators who were aware of the system never reached the stage of considering certification, with a notable share responding that they "don't feel the need" or "never considered it." It suggests a large gap exists between the two stages of recognizing the certifications and of considering or actually obtaining them.

<Key opinions from respondents>
[I heard about them for the first time]
- I learned of GCBPR for the first time. We have never considered certification for cross-border transfers.
- I learned of GCBPR for the first time. We have never considered third-party certification (including for cross-border transfers).

[Have heard of the names to some extent]
- I had seen the names when checking the assessment body's website, so my level of awareness was limited to just having heard of them.
- I was just put in charge of personal information six months ago, so I have only heard of them. Having received this inquiry, my assumption is that they are likely trying to create a common system of sorts.

[Have obtained information through seminars, etc.]
- I participated in a GCBPR seminar. I felt I needed to be properly educated around the time overseas business collaboration began, so I attended. However, my level of understanding remains limited to simply having heard about them.

Q4. Do you know that the names of CBPR-certified organizations are published on the websites of the competent authorities for the CBPR certification system (the Personal Information Protection Commission and the Ministry of Economy, Trade and Industry) as well as the assessment body (JIPDEC), etc.?

[Overview]
Only one business operator was aware beforehand that names of certified organizations were being made public, and the majority of business operators were not aware, or learned about it for the first time as a result of the interview.

Level of recognition was broadly classified into three categories.

First, business operators that had known for some time.

Second, business operators that said the interviews prompted them to become aware.

Third, business operators who had absolutely no knowledge of it. The second and third patterns accounted for the majority, and it became clear that information concerning names of certified organizations being disclosed was not sufficiently available to business operators.

<Key opinions from respondents>
[I've known for some time]
- I do know about it. (Had looked up the system upon receiving newsletters, etc. from the assessment body, and was made aware of certified organizations being disclosed through that process.)

[Learned about it for the first time as a result of the interview/ had absolutely no knowledge of it]

- I am in the process of beginning to look into it after being approached for this interview. We have only just learned that the names of about four certified organizations are publicly disclosed by the competent authorities and assessment body, etc. and we have started reviewing past reports, etc. We have not yet reached the point of having an accurate understanding.
- I didn't know about it until I checked the URL provided by email prior to this interview.

Q5. What is the reason your company has not obtained Global CBPR or APEC CBPR certification?

[Overview]

The reasons certification has not yet been obtained were found to be the combined effects of several factors.

The most commonly cited reason was "I do not feel the need for it in our business," which was based on the perception that there is no direct exchange of personal information with other countries, or that it is very limited. The second most common reason was "lack of awareness and understanding," and this was the case in which respondents did not know of the systems, or even if they did, a detailed understanding was lacking. There were also several comments that the benefits were unclear and that the cost-effectiveness was not apparent, indicating difficulty in explaining to management and the company the specific benefits that would be gained through certification.

In addition, there were cases in which Japanese subsidiaries of foreign business operators expressed concern about the potential impact on their headquarters, an issue specific to Japanese subsidiaries. Others felt that certifications were irrelevant to their company because they perceived certification as being intended for large corporations.

Meanwhile, some business operators that were SaaS users commented that their company is in a position of using the services, and that certification should be the responsibility of SaaS providers. An opinion was also expressed that they did not understand what the benefits of acquiring Global CBPR were for their company, highlighting the need to promote a better understanding of the system.

<Key opinions from respondents>
[Do not feel the need for it in our business]

- We do not gather personal information from customers in principle, and do not handle personal information other than for management of internal information. Therefore, we do not feel the need for certification on a global scale.
- Our business model involves providing Japan's personal information to overseas destinations, but we do not collect personal information from overseas. Therefore, our understanding is that certification does not apply to us at this time. However, we are aware that there is a possibility that this will be necessary in the future, and we are paying close attention to developments.

[Lack of awareness and understanding]

- In the use of cloud services, some employees are in fact aware of personal data undergoing cross-border transfers, but this awareness is limited to only a few individuals and is not recognized by the company as a whole.
- Aside from not having been aware of it, I conducted research after hearing of it. I thought about whether we should obtain the certification or whether the contracted party should. My understanding is that the contracted party should obtain it.
- The main reason was that we were not aware of such certification. Our company is in a position of being the service user, and does not yet fully understand the need for certification. If SaaS providers are certified, we can choose those services. It is not yet clear for us what benefits the company will gain by obtaining certification ourselves.

[Benefits are unclear and the cost-effectiveness is not evident]

- The benefits are not clear. We are considering cost effectiveness of other certifications as well, so without compelling advantages we will likely not obtain it.
- We do not know the extent of the impact that will result relative to cost and effort. Considering the costs of system development, procedures, recertification fees, etc., it is impossible to decide whether to become certified when the results to be gained are unclear.

[Situation specific to foreign business operators]

- Since headquarters is located overseas, there are concerns about the impact on headquarters if the Japanese subsidiary independently becomes certified. We could be challenged for acting on our own, and it is easier as a subsidiary to handle the matter after receiving instructions from headquarters.

[The impression that it is intended for large corporations]

- There is an impression that certification is something obtained from major corporations. Even by looking at the four companies that are certified, it feels unrelated to our company, since the business operators certified are of a completely different scale.

Q6. What is the most important determining factor if considering certification?

[Overview]

The determining factors when considering certification can be broadly classified into three categories.

The first is "external factors and business necessity." The most common response was that companies would consider certification if required by external parties, such as requests from customers, inclusion as a business transaction requirement, or as an eligibility requirement for

contract bidding. This highlights the fact that companies have not considered CBPR certification because they have not received any inquiries from customers or business partners at present.

The second is changes in the business environment and business operations. Some responded that consideration would be made if there were any changes in the company's business environment, such as restarting overseas transactions, commencing acceptance of overseas customers, and taking care of work that requires handling of personal information within the company.

The third is alignment with existing certifications and alleviation of additional work required. Business operators that already have the PrivacyMark and other available certifications said that it would be easier to consider CBPR if there were substantial overlap and minimal additional documentation or operational burden.

In addition, Japanese subsidiaries of foreign business operators indicated that it would be easier for them to address the matter if they were to receive instructions from their headquarters, which is a situation that is unique to group companies.

<Key opinions from respondents>

[External factors and business necessity]

- A determining factor would be the need to become a certified organization to meet a business transaction requirement. If the benefits in relation to the contract are not clear, a decision to obtain certification will not be made.
- We would put it under consideration if a customer requests certification. At present, there are inquiries about the PrivacyMark and ISMS from business partners, but we have never been asked about the GCBPR.
- It would probably be about safety measures. It will depend on the extent to which safety measures can be secured by obtaining certification.

[Changes in business environment and business operations]

- It will become necessary when communication with overseas engineers resumes or for work that involves bringing personal information into the company.
- We recognize that when we become able to accept foreign customers, or when the legal system changes, is when certification will become necessary. At present, there is no immediate need.

[Alignment with existing certifications and alleviation of additional work required]

- Because the company is currently certified with PrivacyMark, it is important that gaps with CBPR certification be minimal, or that it can be handled with an extension of current practices. If it is just the number of application recipients increasing but with not much change in the content of document preparation or increase in operating cost, then it will more likely be put under consideration.
- If separate documentation is required for PrivacyMark and for CBPR, multiple documents will need to be prepared which reduces motivation for certification.
- The effect on cost and workload is a determining factor. If the cost-effectiveness is not clear, it is difficult to move it up to the consideration phase.

[Circumstances specific to group business operators]

- Since their headquarters is located overseas, a Japanese corporation may be concerned of impact on headquarters if it becomes certified independently. It is easier for a subsidiary to address the matter if it is asked to obtain certification as instructions from headquarters.

Q7. Please indicate what information, if any, provided by the websites of the competent authorities and the assessment body would facilitate the consideration of obtaining CBPR certification.

[Overview]

Information that business operators seek can be broadly classified into six categories.

The first is information on the certification process, cost, and time. There were many requests for practical information, such as the steps in the process from the application to certification, the preparation that is necessary, required time and cost, etc.

The second is a concrete example showing the case of a certified organization and the benefits they received. There were many requests for information on actual cases, to see the industries and sizes of business operators that are certified and what benefits they receive.

The third is the criteria for determining whether certification is necessary for their company. There were comments asking for clear standards and examples of what kind of business operations require certification.

The fourth is publicizing the fact that SMEs can also become certified. There was an impression that the business operators that are currently certified are mainly large companies, and there was a request for it to be specifically indicated that even SMEs can obtain certification.

The fifth is educational information on the situation surrounding cross-border transfers. It was pointed out that since there is little awareness of unintentional cross-border transfer due to the use of cloud services occurring, information pertaining to this matter needs to be disseminated.

Sixth is sorting through the relationship between and priorities among other certification systems. With several certification systems, such as the PrivacyMark, ISMS, and METI's security rating system in place, it is difficult deciding which certification should be given priority. Business operators with limited funding and human resources, in particular, indicated that prioritizing would be easier if they had information on the relationship between CBPR and other certification systems, and whether they were differentiated for globally expanding business operators or for domestic transaction-oriented businesses.

<Key opinions from respondents>

[Information on the certification process, cost, and time]

- It is desirable for specific information such as cost, time, and status of certification in other countries to be included. It will be useful for business operators newly becoming certified.

[Concrete example showing the case of a certified organization and the benefits that they received]

- It is helpful to find information about the benefits that a certified organization has actually received and those they found helpful.
- Learning which other companies in the same industry are certified can also be a source of persuasion. The mindset to conform, if "everyone" is getting certified, can also be a factor in the decision to obtain certification.
- Posting reports on what kind of business operators participated in seminars and what opinions were presented can also provide an understanding of the aims of similar-sized business operators.
- It may help business operators further their own study into certification if they were provided specific information that helped other business operators as they stumbled during their process of consideration.

[Criteria in determining whether or not it is necessary for their company]

- Having examples of business fields and business operations that require certification would be helpful.
- It would be good to have clear criteria and case examples that show what conditions absolutely require certification.

[Examples for SMEs]

- A look at the business operators currently certified gives the impression that they are all big corporations, so it would be helpful knowing the scale of business operators that are certified.
- It would be easier to understand if information showing that SMEs can also be certified were to be not only in text-form, but also through the introduction of actual business operators and their comments, as well as the use of diagrams and illustrations.

[Educational information on the situation surrounding cross-border transfers]

- I did watch an introductory video on the JIPDEC website. It would be good to have information posted on the website in document form in addition to the video.
- An issue more fundamental than an explanation of the certification system is the extremely low awareness of cross-border transfer of information occurring when using cloud services. It is easy for business operators with overseas locations and transactions to understand, but it is not understood by business operators that operate only in Japan. This fact needs to be communicated.
- We have a contract in place with a consulting firm, but they have never once mentioned the start of such certification. If there is information dissemination from the assessment body to consulting firms, it may accelerate information being received by business operators.

[Sorting through the relationship between and priorities among other certification systems]

- For a business operator already holding the PrivacyMark, information is needed on what is additionally required and what can be covered outside the scope of the PrivacyMark assessment.
- We would like information on what should be prioritized, among METI's security rating system and several other available certifications. With financial and human resource constraints, it would be easier to prioritize systems if information were divided for companies that are expanding globally and for companies that mainly deal with domestic transactions.

Q8. Can the following be incentives for certification?

[1] Publishing the names of business operators on the websites of competent authorities and the assessment body

[Overview]

While nearly all of the nine business operators did acknowledge it as effective, their evaluation was mixed.

Positive opinions included comments that: it would help promote reliability of the company externally; lead to a sense of security for customers; and also be used within the company to raise awareness of efforts. In particular, business operators that have already experienced the benefits of their name being published with the PrivacyMark responded that they could expect the same results with this certification.

On the other hand, there were some cautious and conditional opinions pointed out, such as: name disclosure alone would not be a significant advantage; it would be an incentive if overseas

transactions were being carried out on a full scale; and it would be meaningless if it were not published on a website that those overseas are able to access. Several commented that, since there are no inquiries coming in at present regarding CBPR from business partners, they would not be able to appreciate any real benefit from disclosure.

<Key opinions from respondents>
[Would be an incentive]
- Publication of our company name would be an incentive. We have created a special page on our company website featuring GCBPR to appeal to the public. Publishing company names is very effective and we'd like that to continue.
- In addition to disclosing company names, it would be good if companies could be featured in dedicated articles. It would lead to becoming an incentive as it could promote efforts both inside and outside the company (especially for industries that handle customer information of individuals).

[Would not be an incentive]
- It is difficult to determine whether or not it would be an incentive. It would be effective if the website is one that people overseas can check and see the names of business operators that are properly GDPR-compliant. It is important that the environment allows people overseas to easily access information from the websites of the competent authorities.
- Publication of the company's name alone does not offer any significant benefit.

[2] An ecosystem (network) being created for the appropriate handling of cross-border data between certified organizations, competent authorities, the assessment body, etc. through CBPR

[Overview]
An ecosystem (network) being created was positively evaluated by all nine companies. Many expressed their opinion that specific benefits were clearer compared to having the names published as indicated in [1].

Anticipated effects include the use of the ecosystem as a forum for information gathering and sharing, being able to obtain the latest information on changes in overseas legal systems, etc., serving as opportunities potentially leading to new business and partner development, and the possibility of building relationships with competent authorities and other certified companies.

In particular, some businesses faced with the problem of difficulty in keeping track of overseas legal systems said that it would be very useful if there were opportunities to share information on legal amendments. Expectations were also expressed as to being able to obtain knowledge of first movers through the network such as during the stage of considering certification.

<Key opinions from respondents>
[Would be an incentive: Anticipated effects]

- It would be desirable to have opportunities to meet with the competent authorities at seminars, etc. and to be able to communicate with them. Having an ecosystem with businesses that recognize the importance of data is also desired, and that may help develop new business.
- Horizontal ties can trigger new business. Since we have transactions with government agencies, obtaining certification will help them feel secure about us as a contracted party and it may lead to events and new orders.
- We would very much appreciate materialization. Please provide information such as guidance from the assessment body, reports on events and meetings held, and participants' reports, etc. including online sessions. Being provided briefing sessions and the like where we can see the kind of networking activities being carried out will help us feel the momentum.
- We need to learn about examples and case studies, so if there are similar cases, it would be helpful to us in understanding the authorization required and what should be observed.

Q9. Are there any other companies in the same industry or business partners (including overseas business operators) that have obtained the Global CBPR/APEC CBPR certification?

[Overview]

It became clear that an understanding of the certification status of other companies in the same industry and business partners is at an extremely low level.

Responses were broadly categorized into three categories.

First, the most common response was "I do not know at all, I am not aware."

Second, some companies responded that they looked into it but could not find any relevance with their own company.

Third, a portion of the companies said that they were aware of the certified companies but did not deal directly with them.

Several respondents said that CBPR was not part of the criteria for selecting business partners or evaluating contracted parties, highlighting the fact that certification is not functioning as a prerequisite for transactions at present.

<Key opinions from respondents>
[I do not know at all, I am not aware]
- Even if we protect personal information within our own region, there is the question of how the matter is being handled overseas, and we wonder whether our partner university overseas is certified.
- I do think that some of our business partners are certified companies, but I have never properly checked. In addition, whether or not business partners are certified is not specifically included in our selection criteria for contracted parties.
- We have never asked about certification among other companies in the same industry, so I don't know. I wonder whether large corporations in the same industry are certified.

[Have looked into it but could not find any relevance with our company]
- I quickly checked, but it is not yet clear. There does not seem to be any direct relevance with our company. Businesses that are certified are such large companies that they do not serve as reference, since our company is not at such a level.

[Are aware of certified companies but do not directly deal with them]
- I often hear the names of Japanese certified companies. We have no direct transactions with them, but they are businesses that we could recognize a connection with.

[Other]
- When viewing the video provided, there was a part that introduced overseas operators that are certified, which did include some of our business partners.

Q10. Do you think that Global CBPR certification is effective (needed) for business operators?

[Overview]

Responses were obtained from all nine companies that were interview targets this time. The assessment of the effectiveness and necessity of GCBPR greatly varied among business operators, depending on the type of business and the degree of foreign involvement.

Responses were broadly categorized into three categories.

First, favorable evaluation as being effective. These were business operators with large transactions overseas or that had already become certified.

Second, evaluation as effective but conditionally. A position taken that it is effective for companies with overseas transactions and for certain industries, but that they do not feel a direct need for it themselves.

Third, companies responded that it is not needed for their company. Some reasons given were that direct exchanges with foreign countries are limited, and that even if certified, they would still be subject to questionnaires during the service provider selection process.

Some companies engaged in business for public entities also expressed the opinion that public entities are often particularly strict about information management, so being certified will serve as external explanatory material, suggesting that the effectiveness of certification increases depending on the industry and customer traits.

<Key opinions from respondents>
[It would be effective]
- The scope of the area covered by GCBPR has expanded, and it is considered to be effective from the viewpoint of enabling smooth flow of data with many businesses and target areas. Being able to skip some contracts and verification work leads to greater efficiency.
- Certification can reduce legal risks not only domestically but also globally. It is effective in differentiating companies from competitors by improving reliability.
- I believe it is effective as evidence of a business partner maintaining a certain level in their management system for handling personal information. The PrivacyMark is limited to the domestic market, so if this certification can be used for evaluation overseas as well, it will make selecting business partners easier, and be effective in that regard.

[Effective but conditionally]
- I think there are certain situations in which it is necessary for the business purposes. In particular, it would be better to obtain certification at least for operators who have exchanges with the European region.
- I think it is effective for companies that often face opportunities to handle personal information through overseas transactions. Manufacturers and other businesses that handle a variety of products should be certified.
- It's about having a good balance with the size of the organization. Effectiveness may depend on the size of the company.

[Not needed for own company]
- I don't think we need it that much. The reason is we have very limited transfers overseas. The company does not have a subsidiary overseas, and I believe it will not have very much impact.
- External audits subject us to questionnaires regardless of whether or not we are certified.

Q11. What are the benefits and drawbacks of Global CBPR certification /APEC CBPR certification when compared with GDPR and other regulations and laws (e.g., adequacy decision/BCR/SCC)?

[Overview]
Responses were obtained from all nine companies that were interview targets this time, but only a limited number of companies were able to clearly respond regarding a comparison between regulatory and certification systems. Many operators responded that they had not considered the issue in detail, that they had never made comparisons, and that they did not understand it. This shows that the GDPR and various cross-border transfer tools are not fully understood.

When comparing regulations with third-party certification, the benefits include objectively verifiable reliability through certification based on third-party assessment, a visualization of the legal compliance status, and ease of explanation to overseas business operators. On the other hand, cost-effectiveness, labor required for operations, and support for certification not being as established as other certification systems, etc. were pointed out as issues that hinder certification adoption.

<Key opinions from respondents>
[Benefits of GCBPR]
- The greatest benefit is that it helps objectively show that a company is certified by a third party as being secure and reliable.
- It helps show that business partners meet a certain level of standard, making the selection of business partners easier. It is beneficial in demonstrating to overseas business operators, who are not well versed in Japanese systems, that standards with common rules are being met.
- I have a sense of lacking knowledge regarding laws in various countries, and not knowing what to do. A globally unified certification would help determine a business operator as reliable if they are certified, so having unified certification is welcome.

[Drawbacks of the GCBPR]
- Cost effectiveness can be included as part of the drawbacks. Currently, the number of participating members is limited, and opportunities for use is limited. I am hopeful that the number of countries, regions, and business operators that are covered will increase.
- It is not so much a drawback, but we don't know in detail how much is involved in operational maintenance and it appears to be quite burdensome. It looks as though a lot of work will be required to get certified. In addition, consultants who can provide support may be few. SMEs are unable to allocate human resources to this and find it difficult to secure personnel.

[Comparison of regulations with third-party certification]
- Laws must be observed. I recall quite a commotion when the GDPR was introduced in 2018, and we studied it exhaustively to become compliant. However, the need for third-party certification varies from company to company, and even if certified, it is something that needs to be maintained.
- Laws must be observed without a doubt, so there is a tendency to continue even at some cost. On the other hand, it is sometimes hard to reach that point in the case of certification systems. There is difficulty in explaining internally why it is necessary.

[Opinions indicating a lack of understanding]
- I don't know, to be honest. I recently learned that there are many different kinds. I have never tried comparing them.
- It is hard to give a clear answer because I do not correctly understand the substance. I am unclear even as to what extent the GDPR covers.

Q12. Have you obtained any certifications excluding CBPR?

[1] Name of certification systems

[Overview]

All nine companies that were interview targets had some kind of certification. The PrivacyMark was most commonly obtained, with eight out of the nine companies certified. ISMS (information security management system) followed, with several business operators certified, and there was a tendency for certification to cover the entire company or some divisions. In addition, some companies held ISO[9] 9001 (quality), ISO 14001 (environment), and PCI DSS (security standards in the credit card industry).

[9]International Organization for Standardization: (ISO) (hereinafter referred to as “ISO”)

It was also confirmed that some businesses that are engaged in public works possess a QMS (quality management system).

<Key opinions from respondents>
- We are a PrivacyMark certified business.
- We have the ISMS, PCI DSS and PrivacyMark certification.
- The PrivacyMark has been obtained company-wide and ISMS by business division unit.
- All business divisions have obtained the ISMS.
- We have group certification for ISO 9001 and 14001.

[2] Reasons for obtaining certification

[Overview]

The reasons for obtaining certification were broadly classified into three categories.

First, the need as a business transaction requirement or as an eligibility requirement for contract bidding. Many cited customers and business partners requiring them to be certified or government agencies requiring it to be eligible for bidding.

Second, as evidence to show reliability and appropriate level of management standards as a business operator, by demonstrating an appropriate management system for personal information and information security externally.

Third, to comply with the legal system. Some business operators were motivated to become certified after the enactment of the Act on the Protection of Personal Information.

<Key opinions from respondents>

[Business transaction requirement, eligibility requirement for contract bidding]
- As the company is entrusted with handling of personal information from customers, it is a transaction requirement that the company is a PrivacyMark certified business.
- The reason is that we get many public sector jobs. It is sometimes an eligibility requirement for bidding.
- When submitting a bid for a tender for translation projects, ISO 27001 is very often a prerequisite. We decided to become certified because it appears that the larger the project scale, the more likely it is to be a requirement for bidding.

[Evidence to show reliability and appropriate level of management standards as a business operator]
- Our company's representative at the time decided to obtain ISO 9001, 14001 and the PrivacyMark all at once. The aim was to demonstrate an appropriate level of management standards as a business operator.
- Because of the large amount of personal information handled in business activities, it was basically considered necessary and therefore we became certified.

[3] Effects of the certification systems

[Overview]

The most common effect of the certification system was having a competitive advantage for transactions and bidding. In many cases with government agency projects and transactions with large

corporations in particular, being certified was a requirement for participation or part of criteria for evaluation. Strengthening internal governance and raising employee awareness was next cited, recognizing the effect of establishing an organizational management system through the process of obtaining and maintaining certification. On the other hand, it was also pointed out as issues that certification has become the norm which diminishes the effect of differentiation, and that the burden of responding to inquiries from business partners is growing.

<Key opinions from respondents>
[Effective]
- Because we have a large number of government agency projects, there are cases in which we need to have the PrivacyMark, ISO, ISMS, etc. to be eligible to bid. Therefore, it is highly effective obtaining such eligibility for bidding.
- Having the PrivacyMark has helped ensure governance and unify awareness among employees.
- Depending on the customer, the methods and systems we use in handling their data, along with the status of regulations development and penalties in the event of an accident, are verified by being audited. Such aspects are covered by having the PrivacyMark and is thus effective.

[No effect felt]
- Lately, most business partners have PrivacyMark as well, so it does not feel very effective.
- Regardless of being certified under the system or not, the process of exchanging information security questionnaires with business partners is becoming complicated. Even if certified, we are subject to surveys, so being certified does not relieve us of that.
- While small-scale businesses with around 20 employees have even obtained certification, there are many cases where big corporations are not yet certified. The low level of social recognitions is a challenge.

[4] Request for improvements in application procedures and operations after certification

[Overview]

Improvement requests were broadly classified into four categories:

First, the digitalization of applications was cited, and there were requests for a change from paper-based to online applications.

The second issue was prior dissemination of information regarding legal amendments, with opinions that it would be helpful to have prior announcements of changes to laws during the review period.

Third, reducing the burden of renewal. There were expectations for a mechanism that would review only differences from the previous fiscal year and reduce the workload according to the number of consecutive years of certification.

Fourth, it was pointed out that greater social recognition of the certification system requires social support.

On the other hand, some responded that there were no particular requests for improvement and that the system is well-developed.

<Main improvement requests among companies>
[Digitalization of applications]
- Would like the application process available in data form instead of on paper. The entire company is managed by data, and output and filing become necessary just for this application. Please digitalize the process.

[Prior dissemination of information regarding legal amendments]
- It would be helpful to receive information in advance as to what legal amendments have transpired over the two years since the previous assessment that we need to pay attention to.

[Reduced burden of recertification]
- We would appreciate man-days required for recertification being gradually reduced. It is better if the system were designed and operated so that only the differences from the previous fiscal year can be closely checked.
- It feels as though there is not much consistency among the assessors in the certification assessments. There is an impression that the content from previous assessments is not being carried over. Feedback included a comment asking what we did in the previous opportunity for improvement. It would be better if there were a mechanism in place to continue building the framework together.

[Social recognition of the system]
- The number of business operators that have Privacy Mark certification should be further increased. I feel social support is necessary for that. With the case of CBPR certification as well, effectiveness of the system is likely attributable to a synergistic support structure.
- I hope that a system is created that allows society to recognize the benefits of this certification.

[5] Future plans for the certification

[Overview]

Regarding future plans for certification, the majority of respondents said that their current status is sufficient or that there are no plans to become certified. However, several business operators were considering obtaining or expanding ISMS. The reasons were that there are more occasions when business partners ask about ISMS, and when ISMS is an eligibility requirement to participate in bidding. On the other hand, it has become clear that securing human resources for certification is an issue, and companies have not taken action to become certified despite recognizing the necessity to do so. Their stance shows reliance on external factors, such as in saying they will consider certification if requested from customers.

<Key opinions from respondents>
[Scheduled to obtain certification (including consideration currently underway)]
- We are considering the timing to obtain ISMS for the entire company. There is concern over business partners becoming more demanding in asking about certification and feel it will likely become necessary.
- ISMS does come up for consideration from time to time. If ISMS becomes an eligibility requirement for bidding when starting a service, we have to seriously consider it.
- The value of certification is primarily its promotional effect, and substantive benefits are significant, such as eligibility for additional bidding points (also considering obtaining Platinum Kurumin certification, which is unrelated to personal data and security).

[No plans to obtain certification]

- No plans at the moment. However, if requested by customers, it will need to be considered for transactional purposes.
- Currently, I am not aware of plans whether or not to renew PrivacyMark or ISMS or to obtain a new certification. We will likely work toward obtaining any certification for a system we feel is necessary.

Q13. What do you most expect from third-party certification systems, including CBPR certification and others?

[Overview]

Responses were obtained from all nine companies that were interview targets this time. The effects expected from third-party certification systems can be broadly classified into four categories.

First, the most common response was to prove credibility externally and provide a sense of security. Expectations were high for the company being able to objectively demonstrate to its business partners and customers that it has an appropriate management system.

The second was the facilitation of transactions and contracts. It was hoped that certification would reduce the amount of investigative responses and verification work required by business partners, and facilitate smooth progress of business.

Third, the responses cited maintaining and strengthening of internal governance. There were expectations that regular reviews would prevent operations from becoming a mere formality and lead to continuous improvement.

Fourth, there were expectations for institutional incentives. Some respondents called for specific incentives for certification, such as reduced reporting for data leaks and benefits in government procurement.

<Key opinions from respondents>

[Prove credibility externally and provide a sense of security]

- A sense of security for customers and business partners is most important.
- Contracts that get renewed and customer confidence are important. The PrivacyMark is generally considered to be highly reliable.
- Third-party certification is a proof that we are handling data correctly, and would therefore like for it to serve as a meaningful and tangible assurance.

[Facilitation of transactions and contracts]

- Ideally it would be sufficient reassurance to respond to contracted party and business partner surveys to state that we are certified. (Currently, even if certified, we need to respond to business partner surveys.)
- When requesting the outsourced vendor to undergo a questionnaire, etc., having the PrivacyMark presented leads to recognition that they are appropriately handling personal information. If they do not have it, it is necessary to confirm the specific management system and regulations one by one, increasing management costs, so effectiveness in this respect is significant.
- It is important that business partners recognize our company to be sound and that there are no problems in the way information is being managed. We hope it will lead to more work opportunities which would be ideal from a business standpoint. It is to promote our reliability.

[Maintaining and strengthening internal governance]

- Regular reviews are effective in preventing operations from becoming a mere formality. Whether operations are being properly carried out can also be checked. I have hopes it serves to ensure security within the company.
- It is raising awareness within the company. There is a sense of being monitored and inspected, which leads to a tendency to do things properly and an awareness of needing to keep it going.

[Institutional incentives]

- In addition to reliability standpoint, we believe there should be benefits such as reduced reporting for data leaks, relief measures, and benefits in government procurement, etc. for having obtained third-party certification.

Q14. This is regarding GCBPR group certification, which is not available in Japan.

[1] Japanese subsidiaries: If you have domestic subsidiaries, would it motivate you to obtain CBPR certification if the system allowed subsidiaries to be certified together with the parent company motivate you to obtain in obtaining CBPR certification?

[Overview]

Six out of nine companies gave positive evaluations of group certification for domestic subsidiaries, as potentially becoming motivation or as being better to have. The main reasons for this were reducing the burden of obtaining and maintaining certification at individual companies, improving the efficiency of group governance, and lowering the hurdle of certification. In particular, some business operators that have already experienced group-certification in ISO and other systems expressed hopes of achieving the same effects.

On the other hand, one company cautioned that the parent company and its subsidiaries often have different perceptions of personal information, so standardization in the group will not reflect the actual circumstances. Thus, certification on an individual company basis leads to more genuine trust. In addition, if a subsidiary has not obtained the PrivacyMark (and other certifications), it is necessary to treat intra-group exchanges in an overly formal manner even though it is within the group, leading to additional work. There was expectation placed on group certification in helping to reduce the burden of information sharing within the group.

<Key opinions from respondents>

[Will be the motive for certification]

- Back when our subsidiaries had the PrivacyMark, it was a heavy burden separately obtaining it for individual companies. It was almost the same package, but it took twice the effort. Group certification would be extremely beneficial.
- Some subsidiaries conduct research. If certification can be obtained as a group, the administrative burden on the group as a whole will be reduced. In the case of quality and environment-related certifications, the same effect can be expected because group companies are collectively applying for certification.

[Will not be a motive for certification]

- Personally, I am against it. Often the degree of perception regarding personal information differs greatly between the parent company and its subsidiaries. A unified group certification system will lead to expansion of the system, but it will not reflect actual circumstances. Each company gaining trust on an individual basis is more genuine.

[2] Overseas subsidiaries: If you have subsidiaries overseas, does the operation of the certification system to include subsidiaries being certified together with the parent company lead to motivation in obtaining CBPR certification?

[Overview]

Group certification for overseas subsidiaries also received generally positive evaluations. In particular, some business operators with overseas subsidiaries expressed the opinion that certification dealing with global cross-border transfers, including overseas subsidiaries, is more consistent with the original intent.

However, there were also practical concerns, such as the feasibility of an effective management system for overseas subsidiaries and it being difficult to maintain from a geographical distance perspective. Several business operators indicated awareness of the challenges in thoroughly implementing policies and maintaining management systems for overseas subsidiaries compared to domestic ones.

<Key opinions from respondents>

[Will be the motive for certification]

- We do not recognize differences between domestic and overseas subsidiaries. With the start of this system, benefits and drawbacks will be taken into consideration and we will choose it if worthwhile. It is a benefit to have the option.
- Overseas group companies likely require this certification most, so it would be easier to handle if certification could be obtained by the group as a whole.

[Will not be a motive for certification]

- Domestic subsidiaries are easier to manage with the short distances, but with overseas subsidiaries, the feasibility of maintaining the management system is questionable.

[3] Do you think it would be better to have group certification, regardless of whether you have subsidiaries?

[Overview]

Regarding the need for a group certification system, six out of the nine companies responded that it would be better to have. The reasons for this included improving the efficiency of cost and labor, lowering the hurdle of certification, and expanding options. In particular, there was an opinion that working together as a group would create greater momentum, and it would be easier to get certified by cooperating with each other.

On the other hand, some voiced their desire for flexibility to be able to choose between group certification and individual company certification. It was pointed out that because cultures and business activities may differ among business operators even within the same group, a system that allows businesses to choose based on their circumstances would be preferable to having group certification uniformly imposed.

In addition, for operational issues related to group certification, requests were made for specific cases to be addressed, such as when conditions do not align due to rules for the parent entity being applied directly to subsidiaries, or cases where partial customization is necessary or it is preferable for assessments to be conducted on a subsidiary basis rather than by business site.

<Key opinions from respondents>
[It would be better to have]

- It would be easier to obtain for companies in a group together rather than individually if they cooperated with each other in terms of costs and labor. The hurdle of certification might be lowered.
- The best choice should be made based on improving the efficiency of internal resources. Companies could choose to be certified on an individual company basis. It is better for each company to have a choice.
- We have ISO certification as a group, so if the parent company suggests group certification, it will be easier to proceed.
- If those within a group are free to choose, then companies with similar cultures can choose group certification, while others can choose individual certification. Such flexibility should help alleviate administrative burden for the group as a whole, and performance can be better controlled.
- We are also promoting the standardization of current policies with affiliated companies, and it would be advantageous to have the option of using this system to make group governance effective.

[Against it /Cannot say either way]

- Even within the same group, there may be differences in the way personal information is perceived, and without adequate education, there is a risk that it will become a mere formality.
- Conditions may not match when rules for the parent entity are applied directly to subsidiaries, so being able to partially customize rules would make it easier.
- As a subsidiary, it is hard to judge because it is up to the parent company. But since it leads to savings in labor and other costs within the group, there may be an opportunity to consider this issue in the future.

Q15. This is regarding GCBPR PRP certification, which is not available in Japan.
[1] Will you be motivated to obtain CBPR certification if PRP certification is initiated?

[Overview]

Whether or not PRP certification (certification for data-processing companies) would be the motivation for CBPR certification was largely divided, depending on the standpoint of the business operator (controller or processor).

Business operators who are controllers (data administrators) expressed the opinion that it does not motivate their company to obtain certification, but a contracted party having PRP certification would serve as a factor in the selection process. Meanwhile, business operators who are processors (data processors) were cautious and said it would not become a strong motivator for them, although they would put certification under consideration if requested by customers.

<Key opinions from respondents>
[Will be the motive for certification]
- It could be an incentive for companies to pursue certification.
- As we are in the cloud business field, I believe we fall under a business operator that requires certification.

[Will not be a motive for certification]
- As a controller, this does not motivate our company to become certified, but it would be desirable for the client to obtain such certification.
- As a processor, we have no plans for certification unless requested by a client.
- Being in the position of a processor and potentially not being able to obtain it even if we wanted to.

[2] Do you think it would be better to have PRP certification, regardless of whether you are a processor or not?

[Overview]
The majority of respondents said that the need for a PRP certification system should be met, but conditions or reservations were attached in many cases.

Positive comments said it would help distinguish and manage contracted parties and business partners, serve as evidence that processors are in legal compliance, and that having more choices will be beneficial.

On the other hand, there were concerns such as the need for multiple certification if serving as both controller and processor, difficulty in segregating them, and not knowing what effect can be gained if recognition level is low. Others said that it would be better if both aspects could be covered with one certification.

<Key opinions from respondents>
[It would be better to have]
- From the viewpoint of managing contracted parties and business partners, such certification makes it very easy to distinguish them.
- Having a system is preferable because a contracted party that has Global PRP serves as a factor in the selection process.
- It is worthwhile if it proves our company's legal compliance as a processor. However, it is hard to tell its effectiveness if recognition is low, so we will put it under consideration after looking into the cost and effort required.

[Cannot say either way]
- It is likely easier to manage for business operators that specialize in data processing. In our case, however, because business operations involve both controller and processor functions, multiple certifications are needed, and the actual benefits are limited.
- Dividing the systems may cause changes in audit methods, but since our company both entrusts and subcontracts work, I would wish obtaining one certification would address both perspectives.
- Honestly speaking, I don't really know. It is difficult to draw a line in determining whether to obtain Global PRP or to consider PrivacyMark and other similar systems as being sufficient. I find it hard to imagine whether our company's own servers would need to obtain Global PRP, or whether the certification held by providers of the cloud services that we use would be sufficient.

Q16. This question involves the expansion of Global CBPR certification in Japan.

[1] What methods do you think are effective in raising awareness?

[Overview]

We were able to get concrete proposals from all nine companies for effective ways to raise awareness. Responses were broadly divided into six categories.

First, the most common response was the clarification of specific benefits and cost effectiveness. There was a shared awareness that the key to encouraging a shift from recognition of certification to considering obtaining it is clearly indicating what can be gained by becoming certified.

Second was introducing examples of certified organizations. The opinion was expressed that showcasing successful cases of business operators in the same industry and of the same scale, and publicizing the fact that certification is also possible for SMEs, would be effective.

Third was leveraging ripple effects from large corporations. Major companies taking the initiative in obtaining certification and asking their business partners to also do so would help rapidly spread the adoption of certification.

Fourth, raising awareness of the relationship between the use of cloud services and cross-border transfers. It was pointed out that greater awareness is needed of cross-border transfers actually occurring with the use of cloud services, even by those who believe that their business operations are being carried out only in Japan.

Fifth, enhancing seminars and information dissemination. It was proposed that awareness-raising seminars and opportunities for exchanges of opinions be provided, and to clarify that the certification is positioned as an additional one for PrivacyMark certified businesses.

The sixth was information dissemination by SaaS providers. There was an opinion that visibility would increase by certified companies publicizing certification. If SaaS providers become certified organizations and promote their status as GCBPR-certified, awareness of it would spread among service users.

<Key opinions from respondents>

[Clarification of specific benefits and cost effectiveness]

- It is important to clearly show the benefits to business operators.
- It may serve as an incentive for companies to take the first step in considering the adoption of the system if they knew about the cost effectiveness. Many companies are under the impression that the system does not apply to them, so it would be helpful to have an indication of how much cross-border transfer activity by a company would make certification advisable for them.

[Introducing examples of certified organizations]

- Successful cases involving well-known companies would make it easier to understand. It would be helpful to have educational seminars and opportunities for the exchange of opinions. Introducing the precedents of not only large corporations but also SMEs would be effective.

[Leveraging the ripple effects of large corporations]

- Large companies should become certified. It would create more opportunities for exposure, and people will likely be interested. If large corporations increasingly seek certification from their business partners, adoption will rapidly spread.

[Raising awareness of the relationship between the use of cloud services and cross-border transfers]

- If companies that use cloud services do in fact need certification, that fact becomes a key point of appeal. Emphasizing the fact that the use of cloud services involves cross-border transfers should be effective.
- It is important to start with spreading awareness that the use of the cloud alone causes cross-border transfers of personal information to overseas countries. I think it would be effective to distribute a video that introduces only that.

[Enhancing seminars and information dissemination]

- If PrivacyMark certified businesses are made aware that they can obtain additional certification, it may be easier for business operators already certified to obtain this certification.
- It is important that the system itself is explained in an easy-to-understand manner. Companies will not reach the point of considering it without sufficient understanding.
  I do not look at all the information available regarding seminars, so eye-catching phrases in seminar titles, such as "XX certification now available!" or "Is your company safe without XX certification?" would be effective. This is because many people do pick up on such titles and then actually go watch them.

[Information dissemination by SaaS providers]

- As a SaaS user, it becomes a point to check when selecting tools if vendors promote the fact that they have GCBPR certification. It would be effective to get business operators that are certified to publicize that fact more widely so more people can see it.

[2] As a measure during the expansion stage, do you think that benefits such as free review fees for a certain period are effective in growing the number of certified organizations?

[Overview]

Evaluation was divided as to the review fee being free of charge. Two out of nine companies responded that it would be effective. Seven companies responded that it would not be effective, with four being of the opinion that it could be effective under certain conditions, such as on a short-term basis and being offered when a company is putting it under consideration.

The seven companies that responded that it would not be effective raised concerns about man-days, labor, and maintenance after becoming certified.

<Key opinions from respondents>

[It would be effective]

- I think it's a very good idea. It would likely be effective if offered to business operators using cloud services in appealing to senior management, for them to take advantage of the opportunity to become certified.
- I think it would be a good incentive. There don't generally seem to be any sale offers for certifications, so the impact would be strong if a "save now" or similar special were made available. Since people don't have that kind of image for certifications, the impact would be quite strong.

[It would be effective under certain conditions]

- The review fee being free of charge for a limited time during the expansion phase may be effective in the short term.

- I think it is effective to a certain extent. However, given the personnel costs and time required, the review fee being free doesn't make it good. It may be worthwhile as a trial attempt.
- Making it free of charge would be effective when companies feel a certain amount of necessity for the certification. Nevertheless, necessity first needs to be established, and if the measure is available when trying to get certified as the system becomes widespread, then it would be effective. The running cost for maintenance also needs to be considered.

[It would not be effective]

- It may depend on the size of the business operator. The incentive will not work in the case of our company. Our stance is to pay for any reasonable costs that are necessary, and just the fee being waived would not be an incentive to obtain certification. But, if it happens to be free at the same time it is being put under consideration, it might help us decide to get certified.
- Unless the benefits are clear, we would not obtain certification even if it were free. Balancing the cost, effort, and benefits of maintenance and upgrading is the key in making the decision.

[3] What do you think needs to be done to make cross-border transfer tools, such as CBPR certification, more appealing to business operators in Japan?

[Overview]

The requirement most often noted for motivating more business operators to obtain certification was the creation of external factors. The majority responded that they would obtain certification if their business could not be carried out without it, such as to meet requests from business partners and eligibility requirements to participate in bids.

This was followed by clarification of the benefits and cost-effectiveness. It was pointed out that the person in charge being able to cite specific benefits to senior management would lead to action toward certification.

Other important factors included certification among large corporations first and ripple effects on business partners, raising awareness about unconscious cross-border transfers, and coordination and improved efficiency with existing certifications.

There was also a suggestion to incorporate assessment for certification into existing ones. Specifically, the opinion was that by checking cross-border transfers during the PrivacyMark assessment, business operators would be compelled to recognize the reality of cross-border transfers and interest in CBPR would grow.

<Key opinions from respondents>

[Creation of external factors]

- External factors are important. It may be too coercive to make it a requirement for government commissioned projects, but business operators will have no choice but become certified with such external factors in place.
- If it is required for those using cloud services to become certified as a condition for bidding, companies will do so out of necessity.

[Clarification of the benefits and cost-effectiveness]

- If the cost-effectiveness is clear, a cycle is created in which the person in charge will be motivated and find a path to approach senior management.
- Knowing about the cost-effectiveness makes it easier to start considering adopting the system. It is helpful to understand that not only large corporations but also SMEs are eligible.

[Certification among large corporations first and ripple effects on business partners]

- It is necessary to learn why large companies do not get certified even though they have exchanges with overseas entities. Most business operators work with large companies, so they will get certified if told it is needed to conduct business.

[Raising awareness of unconscious cross-border transfers]

- A correct understanding of cross-border transfers taking place is first needed. Disseminating information that shows the benefits and drawbacks in an easy-to-understand manner is also needed, by comparing business operators that are certified with those that are not.

[Coordination and improved efficiency with existing certifications]

- If a business operator has the PrivacyMark, it may be easier if parts relevant to that are removed from assessment in obtaining additional certification. If assessment can be carried out at the same time, overlap can be avoided and burden reduced.
- Cross-border transfers have never been brought up with PrivacyMark and were not an issue in the assessment. If CBPR is incorporated into the PrivacyMark assessment and ISO, we will have no choice but to obtain it. SaaS providers becoming more aware of the situation and getting certified should considerably help its spread.

[Questions to the certified organizations]

Business operators that are certified were asked questions in addition to Q1 - Q16 above. An outline of the questions is provided below.

<Additional questions>

Q1. What was the motivation for considering CBPR certification and what was the key factor in becoming certified?

[Overview]

Motivations and key factors cited were the determination that third-party certification was crucial as proof that important customer information is being appropriately handled, since information of users and employees is being handled at overseas locations.

<Key opinions>

- Development bases are also located overseas, and information is being coordinated with them. Data are not only that of employees, but includes user information being handled at overseas locations. In terms of ensuring the appropriate handling of important user information, it was determined that obtaining third-party certification was crucial. Such a perspective was a major factor in the decision to become certified.

Q2. This is to inquire about the GCBPR certification review process.

[1] How many man-days does it take to prepare for certification or recertification (preparation of necessary documents, etc.)? Please tell us if there is anything that is particularly burdensome for the assessment.

[Overview]

It has been shown that preparation for certification and recertification takes a certain amount of man-days. In particular, updating the supporting documentation to be submitted at the time of application and responding to the items pointed out in the previous fiscal year take up man-days, but there is

indication that the first year had the heaviest burden, and the accumulation of know-how led to a tendency for decreased man-days from the second year onwards.

It was also pointed out that the type and content of material to be submitted are unclear as to the extent that should be prepared for assessment to start and become completed, which may be posing a hurdle for business operators considering certification.

<Key opinions>
- We prepare multiple supporting documentation each year when submitting a recertification application. Man-days are required in submitting a recertification application, handling issues that are pointed out regarding the previous fiscal year, etc. I have an impression of it being a burden to maintain.
- There is a reduction in man-days required to prepare documents as we get accustomed to the process and accumulate the know-how. The burden is the greatest in the first year. This is likely one of the factors behind the sluggish number of business operators obtaining certification.
- Preparing the necessary documents to start the assessment is hard without being able to accurately identify what they are. It becomes a hurdle in the process of requesting approval from management.
- Because details of assessment vary according to the type of business and services offered by each business operator, it is difficult to determine the extent to which our company is expected to prepare.
- If the objectives of the certification assessment could be outlined and more document templates/samples provided, it could help alleviate the burden.

[2] Is there anything in the certification review process that you would like to see improved? (Overlap with ISMS)

[Overview]

We looked into the extent to which man-days could be reduced by obtaining ISMS at the same time, and although some documents were common between the two systems, it did not lead to a significant reduction in man-days. This was due partly to internal operational issues, as different departments within the company were handling each of the systems. It was also suggested that by establishing how information assets and personal information should be handled at the time of application, the hurdle for certification assessment could be lowered.

<Key opinions>
- GCBPR and ISMS are being handled by separate departments. Some documents are common among the two and the ledgers to be referenced are the same, but they do need to be processed for the purpose of GCBPR. Thus already having ISMS certification does not significantly reduce man-days.
- In order to prevent unrelated information from being included, all data are checked, partially deleted, and multiple ledgers are consolidated for submission.
- There are many companies that manage information, but there are few companies that manage personal information independently. A successful approach to this would also lead to lowering the hurdle for certification assessment.

Q3. This is regarding the effectiveness of obtaining Global CBPR certification.

[1] In what situations in your business is Global CBPR certification utilized?

[Overview]

Externally, it is effective when starting business with new business partners to present it as proof of our company's reliability. Internally, preparing for certification has led to heightened employee awareness and strengthened the organizational structure.

<Key opinions>

- When starting a business with new partners, it helps create a sense of security as their first impression when we present the certificate as confirmation of our information management system.
- Within the company, employee awareness has changed along with the organizational structure through preparations for certification. GCBPR is being effectively utilized both internally and externally.

[2] Are there any examples of your company having benefited from Global CBPR certification in business-related areas?

[Overview]

Examples of business-related benefits were cited by companies who were provided opportunities to communicate to the public, such as speaking engagements at seminars and being invited to APEC events. In addition, GCBPR certification has been added to their checklist in the selection of business partners, and transactions with certified organizations are actually taking place. It is highly effective as evidence of credibility and in helping procedures move smoothly, for example, by reducing the number of additional items to be checked in the evaluation of business partners.

On the other hand, there was an opinion surrounding risks in the certification system, that simplification of contracts between business operators cannot be achieved by certification alone, since certification systems could potentially be discontinued.

<Key opinions>

- We use it for opportunities to communicate externally, such as through speeches at seminars and invitations to major APEC events.
- In the selection of business partners, our checklist includes items as to whether they have GCBPR certification and a system that is GDPR-compliant, and transactions with certified organizations are actually taking place.
- In actual use, it is difficult for it to enable contracts between business operators to become simplified. Since the certification is recertification-based*, having certification at the start of the contract does not guarantee that it will be renewed later, so there is risk in simplifying the contract based on certification alone.

*The system is based on a recertification application being submitted every year.

[3] As a Global CBPR certified organization, what types of industries and businesses would you like to see obtain CBPR certification?

[Overview]

Respondents expressed hope that in the cloud services sector where many are certified in the United States in particular, Japanese peer companies getting certified would help in the facilitation of services they use.

<Key opinions>

- Because there are many CBPR certified organizations in the United States, we would like similar business operators such as Japanese cloud service providers to prioritize consideration into certification. This will lead to facilitation of services we use.
- Utilization of this system throughout Japan would be helpful as it would allow checklist items to be skipped, improving efficiency and stimulating data flow.

Q4. What are your thoughts as to why Global CBPR adoption has not progressed?

[Overview]

The lack of tangible benefits was cited as the reason for the slow progress.

As a concrete measure to promote the adoption of the system, the creation of tangible benefits was suggested, such as being exempt from reporting data leaks and incorporating the system as an eligibility requirement for government bidding.

<Key opinions>

[Creation of concrete benefits]

- As measures to promote the adoption of the system, being able to present tangible benefits and cost-effectiveness, such as exemption from reporting of data leaks, etc. and clearly positioning GCBPR certification along with ISO and PrivacyMark as an eligibility requirement for government bidding may help spread the adoption of certification.
- Costs are being incurred to research foreign legal systems for cross-border transfers. Increasing the number of countries subject to foreign legal systems researched by the competent authorities and increasing the frequency of updates could reduce the burden on business operators. In addition to presenting the benefits, efforts to reduce the burden on business operators are also effective in promoting adoption.

(7) Summary of survey interview results

This research revealed that the awareness level of GCBPR was low overall. However, the most common reason among respondents for not getting certified is the sense that they do not feel the need for it in their business, based on the recognition that their direct personal data exchanges with other countries are limited. This was followed by a lack of awareness and understanding, with many not reaching the stage of considering it because they were not aware of the system, or lacked sufficient information even if they were.

With regard to incentives for business operators to obtain certification, almost all companies responded that it would be better to have group certification, which has not yet been introduced in Japan, even if under certain conditions, as it would reduce operation and maintenance costs for companies that manage multiple certification systems. Opinion was also provided that Global PRP,

which has not yet been introduced in Japan, can be effective to a certain extent under certain conditions. However, several companies who act as controllers gave their opinion that they would like their contracted parties to become certified, and companies who are processors said they do not feel the need, splitting the overall opinions into two.

External factors and business necessity were cited as the most common determinants in considering certification, and it became clear that external factors are required (selection criteria when starting a new business and eligibility requirement to participate in bidding for administrative commissioned projects), in the same way as motives for obtaining the PrivacyMark and ISMS, which a large number of companies in Japan currently have obtained.

Meanwhile, one company that has obtained GCBPR cited the following points as advantages of certification: the smoothness of new business transactions resulting from proving credibility externally, and the improvement of employee awareness and organizational structure within the company. In addition, a suggestion was provided, given the current issues, to establish preferential measures when obtaining other certifications in order to reduce the burden of applications.

2.3. Detailed Analysis of the Strengths and Benefits of GCBPR

(1) Research objective

The objective is to conduct a comparative analysis of the Privacy Information Management System, or PIMS[10] (hereinafter referred to as "PIMS") and GCBPR program requirements, while also using the findings of the 2024 Research, to clarify the more detailed strengths and benefits of GCBPR compared to other systems.

(2) Research targets

A comparative analysis was conducted between PIMS and GCBPR program requirements, using the ISMS-PIMS certification as evidence that PIMS has been properly implemented and is operating, and the 2024 mapping survey[11] results as analytical targets.

In the 2024 Research, based on the assumption that business operators that are considering GCBPR certification are likely to have already obtained third-party certification for personal information and information security, a mapping survey was carried out with CBPR program requirements for PrivacyMark and ISMS, which have a particularly large number of certified organizations among the major Japanese certification systems. ISMS-PIMS was also identified as a key certification system in Japan in the 2024 Research, but was not included in the scope of the mapping survey because it did not meet the criterion as a certification system that many Japanese business operators had obtained. This was due to its limited number of certified organizations compared to PrivacyMark and ISMS and the fact that ISMS-PIMS was available only to ISMS-certified organizations as an optional extension.

[10]See (3) Overview of ISMS-PIMS and PIMS. Since PIMS became a standard independent from ISMS-PIMS starting October 2025, the mapping analysis in Subsection 2.3 uses PIMS for comparison of research targets, while figures showing actual results, such as the number of certified organizations, etc., use those for ISMS-PIMS.

[11]Refer to the 2024 Research Report, Chapter 2: Activities for Disseminating CBPR, 2.1.2 Mapping Survey (pp. 16-48).

This research covers both ISMS-PIMS and PIMS in order to examine how GCBPR is affected by the transition of PIMS. It has moved from an extension of ISMS, which focuses on information security, to an independent standard that centers on privacy requirements while also covering information security.

(3) Overview of ISMS-PIMS and PIMS

[1] ISMS-PIMS

In recent years, laws and regulations on privacy-related matters, including the GDPR (EU General Data Protection Regulation), are being strengthened worldwide. In order to comply with these laws and regulations, organizations are expected to establish a comprehensive management system for the handling of personal information.

PIMS, based on ISO/IEC 27701, is an international standard for managing risks associated with the processing of personally identifiable information (PII), including collection, use, storage, and modification, and implementing privacy protection. ISO/IEC 27701:2019,[12] published in 2019, extended ISO/IEC 27001, the certification standard for an information security management system (ISMS), and added requirements for privacy controls (hence, the ISO/IEC 27701:2019 conformity assessment scheme is referred to as "ISMS-PIMS").

To obtain ISMS-PIMS, prior ISMS certification is required. In Japan, assessments for ISMS-PIMS began in 2021, and in about four years (as of November 14, 2025), 68 organizations have been certified. Certifications have also been obtained in the United States, China, India, and other countries.

[2] PIMS

In October 2025, ISO/IEC 27701 was revised and ISO/IEC 27701:2025 was published. The revised standard became a management system standard independent from the ISMS certification standard ISO/IEC 27001, rather than an extension of it, in accordance with the ISO Central Secretariat's policy regarding management system standards.[13]

With this, the content of ISO/IEC 27701:2025 has substantially changed from ISO/IEC 27701:2019, to be consistent with other management systems. However, there have not been significant changes in the privacy-protection requirements.[14] The transition period for certification is three years (until October 31, 2028), starting from the end of the month in which the standard was published (October 31, 2025). The timing of this research (November 2025) falls within the transition period for certification.

---

[12] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (based on this International Standard, the Japanese Industrial Standards “JIS Q 27701:2024 Security techniques — Extension to JIS Q 27001 and JIS Q 27002 for privacy information management — Requirements and guidelines” have also been published without technical content and structure being changed.)

[13] ISO has several types of standards, including management system standards such as ISO9001, 14001 and 27001 for organizational operation and management, standards related to products/technical specifications such as ISO26262 and 13485, and standards intended for self-declaration of conformity rather than third-party certification, such as ISO 26000

[14] ISMS Accreditation Center (ISMS-AC) website, “PIMS Conformity Assessment Scheme” https://isms.jp/pims.html

Table 6　Overview of ISMS-PIMS and PIMS

Item	Description
Abbreviation	• ISMS-PIMS (ISO/IEC 27701:2019) • PIMS (ISO/IEC 27701:2025)
Subject of evaluation	• Frameworks for managing the risks associated with the processing of personally identifiable information (PII), including collection, use, storage, and modification, and implementing privacy protection • The scheme covers PII controllers (i.e., privacy stakeholders, excluding individuals who use data for personal purposes, that determine the purposes and means for processing PII).and PII processors (i.e., privacy stakeholders that process PII on behalf of and in accordance with the instructions of PII controllers) • *Common to ISMS-PIMS and PIMS
Relevant laws, regulations, standards, etc.	• ISMS-PIMS: ISO/IEC 27701:2019 "Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines" • PIMS: ISO/IEC 27701:2025 "Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance"
Accreditation and certification bodies	• Accreditation body in Japan: ISMS Accreditation Center (ISMS-AC) • Certification bodies in Japan: 7 (All as of November 14, 2025)[15] * Transition from ISMS-PIMS to PIMS The accreditation body will begin accreditation assessments of certification bodies that will use ISO/IEC 27701:2025 by July 30, 2026. Certification bodies will begin assessments with ISO/IEC 27701:2025 based on the transition date of accreditation and shall use ISO/IEC 27701:2025 to assess all non-certified organizations by October 31, 2028.
Application/certification unit	Organization, department, and service units[16] *Common to ISMS-PIMS and PIMS
Number of certifications	68 registered (65 published) (as of November 14, 2025)[17] *Number of ISMS-PIMS certifications
Recertification period	Three years (annual surveillance audits and a recertification audit every three years) * Common to ISMS-PIMS and PIMS

[15]ISMS Accreditation Center (ISMS-AC) website, “List of ISMS-PIMS Certification Bodies” https://isms.jp/lst/isr/index-isms-pims.html

[16] Although not explicitly stated in the standard, the principle shared by ISO management system standards is that even with the scope of certification being the entire organization, it can be limited to some departments or certain services.

[17]ISMS Accreditation Center (ISMS-AC) website, “List of ISMS-PIMS Certified Organizations” https://isms.jp/isms-pims/lst/ind/index.html

Item	Description
Year of commencement of certification	• ISMS-PIMS: 2021 • PIMS: Starts between August 2026 and October 2028 (Based on the transition date)
Official information	https://isms.jp/pims.html

ISMS-PIMS and PIMS classify organizational roles into PII controllers and PII processors,[18] and define controls. GCBPR offers certification for both controllers and processors, and its assessment scope also covers PII; the two schemes are therefore highly compatible.

(4) Comparative analysis of PIMS and the GCBPR program requirements

GCBPR provides the Global CBPR for personal information controllers (hereinafter referred to as "controllers") and the Global PRP for processors, formulated based on the nine GCBPR Privacy Principles.[19]

The Global CBPR is designed to assist in demonstrating the controller's capability to comply with data-protection and privacy-related obligations. When obtaining Global CBPR, the applicant organization must evaluate its compliance using the Global Cross-border Privacy Rules (CBPR) System Intake Questionnaire, which reflects these program requirements.

The Global PRP, meanwhile, is designed to assist in demonstrating the ability of personal information processors (hereinafter referred to as "processors") to support controllers in complying with data protection and privacy obligations.

To analyze the strengths and benefits of GCBPR, this research conducted a comparative analysis of GCBPR program requirements and ISO/IEC 27701:2025 (PIMS) published in October 2025.

ISO/IEC 27701:2025 is a management system standard that requires an organization to select privacy risk response options and determine all controls required to implement them, taking into account privacy risk assessment results. The organization is required to compare the determined controls to those shown in Annex A of PIMS (ISO/IEC 27701:2025) to verify that the required controls have not been overlooked. However, the organization may add or exclude controls when needed. The control objectives and controls set out in Annex A are organized into those for PII controllers, those for PII processors, and those common to PII controllers and processors.

Accordingly, this research compared and analyzed the GCBPR program requirements with the control objectives and controls for PII controllers in the main text of the standard and Annex A, and the control objectives and controls for PII controllers and PII processors. (However, in practice, additional controls may be included with those in Annex A or controls may be excluded, depending on the results of each organization's risk assessment.) The results are presented in (5).

Similarly, a comparative analysis was conducted for program requirements of the Global PRP with the control objectives and controls for PII processors and those for PII controllers and PII processors in the main text of PIMS (ISO/IEC 27701:2025) and Annex A.

[18] A PII controller is a privacy stakeholder that determines the purposes and means for processing PII, excluding individuals who use data for personal purposes. A PII processor is a privacy stakeholder that processes PII on behalf of and in accordance with a PII controller’s instructions.

[19] Preventing harm, notice, collection limitation, use of personal information, choice, integrity of personal information, security control, access and correction, and accountability.

(5) Comparison with the requirements of the Global CBPR program

The outcomes of the comparison with the requirements of the Global CBPR program are listed below. Program requirements having equivalents are marked "Yes", "No" if they are none, and "Partially" if there are similar requirements but not considered equivalent. For a program requirement that offers options, the question will be marked with a slash unless it can be directly answered, and only the options will be the target of comparison. [20]

[1] Notice

The Global CBPR program requirements for notice require that individuals understand the organization's policies regarding the personal information collected, to whom it may be transferred, and for what purpose it may be used, and that, subject to the qualifications to the provision of notices, individuals know when the personal information is collected, to whom it may be transferred, and for what purpose it may be used.

PIMS also requires the establishment of a privacy policy, and the controls include the identification of purposes, determining the information to be provided to PII principals and providing information.

Table 7 Comparison with GCBPR program requirements for notice

Question	PIMS
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	Yes
a) Does this privacy statement describe how your organization collects personal information?	Yes
b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Yes
c) Does this privacy statement inform individuals whether you make their personal information available to third parties and for what purpose?	Yes
d) Does this privacy statement disclose the name of your company and location, including information on how to contact you about your practices and handling of personal information upon collection? Where YES, describe below.	Yes
e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Yes
f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Yes

[20] The program requirements are structured in a manner that requires some questions to be answered (e.g., Question 1), while others present options to which answers may be given (e.g., Question 5). In the latter case, the comparison column for the question itself is marked with a slash.

Question	PIMS
2. Subject to the Qualifications[21] listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf) do you provide notice that such information is being collected?	Yes
3. Subject to the Qualifications below, at the time of collection of personal information, (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Yes
4. Subject to the Qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Yes

[2] Collection limitation

The Global CBPR program requirements for collection limitation require ensuring that the collection of information is limited to the stated purposes.

PIMS controls also indicate limiting the collection of PII in relation to the intended purposes and identifying legal basis.

Table 8 Comparison with the GCBPR program requirements for collection limitation

Question	PIMS
5. How do you obtain personal information:	
a) Directly from the individual?	Yes
b) From third parties collecting on your behalf?	Yes
c) Other. If YES, describe.	Yes
6. Do you limit your collection of personal information (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Yes
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Yes

[3] Uses of personal information

The GCBPR's program requirements for the use of personal information require ensuring that the use of personal information is limited to fulfilling the purposes of collection and other compatible or related purposes.

PIMS also provides controls, such as identifying purposes and legal basis.

[21] Qualifications refer to "Qualifications to the Provision of Notice" as described on pages 5 and 6 of the GLOBAL CROSS-BORDER PRIVACY RULES SYSTEM (CBPR) PROGRAM REQUIREMENTS MAP https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Program-Requirements_Final.pdf (Hereinafter, the same for program requirements 2 to 4 in this report).

Table 9 Comparison with GCBPR program requirements for personal information use

Question	PIMS
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Yes
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.	
a) Based on express consent of the individual?	Yes
b) Compelled by applicable laws?	Yes
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Yes
11. Do you transfer personal information to personal information processors? If YES, describe.	Yes
12. If you answered YES to Question 10 and/or Question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? Describe below.	Yes
13. If you answered NO to Question 12, or if otherwise appropriate, does the disclosure and/or transfer take place under any of the following circumstances?	
a) Based on express consent of the individual?	Yes
b) Necessary to provide a service or product requested by the individual?	Yes
c) Compelled by applicable laws?	Yes

[4] Choice

GCBPR program requirements for choice require that individuals be provided with choice in relation to collection, use, and disclosure of their personal information.

PIMS also provides controls such as determining the timing of consent, obtaining informed consent, determining the information to be provided to PII principals, and providing information. For Question 19 in the GCBPR program requirements, while PIMS controls seek for information to be provided to PII principals in a clear and easily accessible method, there is no clear reference to it being "affordable" and is thus marked "Partially".

Table 10 Comparison with the GCBPR program requirements for choice

Question	PIMS
14. Do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES, describe such mechanisms below.	Yes

Question	PIMS
15. Do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES, describe such mechanisms below.	Yes
16. Do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES, describe such mechanisms below.	Yes
17. When choices are provided to the individual offering the ability to limit the collection (Question 14), use (Question 15), and/or disclosure (Question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Yes
18. When choices are provided to the individuals offering the ability to limit the collection (Question 14), use (Question 15), and/or disclosure (Question 16) of their personal information, are they clearly worded and easily understandable?	Yes
19. When choices are provided to the individual offering the ability to limit the collection (Question 14), use (Question 15) and/or disclosure (Question 16) of personal information, are these choices easily accessible and affordable? Where YES, describe.	Partially
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary.	Yes

[5] Integrity of personal information

The GCBPR program requirements for the integrity of personal information require ensuring that records are accurate and complete and are kept up to date.

PIMS controls also address accuracy and quality, as well as access, correction, and deletion..

Table 11 Comparison with the GCBPR program requirements for personal information integrity

Question	PIMS
21. Do you take steps to verify that the personal information held by you is up-to-date, accurate, and complete, to the extent necessary for the purposes of use? If YES, describe.	Yes
22. Do you have a mechanism for correcting inaccurate, incomplete, and outdated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Yes
23. Where inaccurate, incomplete, or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	Yes
24. Where inaccurate, incomplete, or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.	Yes
25. Do you require personal information processors, agents, or other service providers who act on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out of date?	Yes

[6] Security safeguards

GCBPR program requirements for security safeguards require ensuring that when individuals entrust their information to an organization, their information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification, disclosure, or other misuses of information.

PIMS likewise requires organizations to conduct risk assessments and to implement risk responses based on the results, and it specifies information security controls.

For comparison with GCBPR program requirements Question 30 c) and Question 32 regarding detecting, preventing, and responding to security failures, PIMS includes references to detecting fraudulent activities through the collection and analysis of logs and is therefore marked "Yes". However, there are no monitoring activities, such as those in ISMS, or controls for acquiring vulnerability information and detecting malware.

For Question 30 d) regarding physical security, ISO/IEC 27701:2019 included controls for physical security perimeters, physical entry, and the security of offices, rooms, and facilities, but these were made N/A in the 2025 revision; the item is therefore marked "Partially".

For testing the effectiveness of safeguards in Question 33, although PIMS specifies the establishment and application of rules for secure development of software and systems related to PII processing as a control, security tests during development and acceptance, among others, are not included as controls and have therefore been assessed as "Partially".

In comparing Question 35 a) as to whether processors of personal information and others are required to implement an information security program that is proportionate to the sensitivity of the information and Question 35 c) as to whether they are required to take immediate steps against security breaches, PIMS controls generally require processors of personal information to contractually support the controllers' obligations. However, the only specific information security control identified was one addressing the implementation of controls over the transmission of PII; the item is therefore marked "Partially". For Question 35 b) concerning the personal information controller being notified promptly by the processor at the time of an incident, while notification is included in PIMS as a concept, there is a lack of reference to its timing and is therefore marked "Partially".

Table 12 Comparison with GCBPR program requirements for security safeguards

Question	PIMS
26. Have you implemented an information security policy?	Yes
27. Describe the physical, technical, and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification, or disclosure of information, or other misuses.	Yes
28. Describe how the safeguards you identified in response to Question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	Yes
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g., through regular training and oversight).	Yes
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:	

Question	PIMS
a) Employee training and management or other organizational safeguards?	Yes
b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?	Yes
c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?	Yes
d) Physical security?	Partially
31. Have you implemented a policy for secure disposal of personal information?	Yes
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Yes
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in Question 32? Describe below.	Partially
34. Do you use third-party certifications or other risk assessments? Describe below.	Yes
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:	
a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?	Partially
b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of your organization's personal information?	Partially
c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	Partially

[7] Access and correction

The GCBPR program requirements for access and correction require ensuring that individuals can access and correct their information.

PIMS also provides controls for handling requests from PII principals, providing copies of PII being processed, and enabling access, correction, and deletion.

For comparison with GCBPR program requirements Question 37 a) regarding confirming the identity of individuals requesting access, PIMS does have controls requiring legitimate requests from PII principals to be addressed; however, no clear reference is made to identity verification, so it is marked "Partially".

For Question 37 d), which concerns providing individuals access to their personal information in a way that is compatible with the regular form of interaction with them, while there are controls in PIMS for a method that is clear and easily accessible to PII principals, it is assessed as "Partially" because there is no mention of compatibility with the regular form of interaction.

Regarding Question 37 e) requesting that the charges for providing access not be excessive, PIMS refers to the fact that fees for disclosure may be legally permitted, but the item is marked "No" because the setting of fee levels is not addressed.

Table 13 Comparison with GCBPR program requirements for access and correction

Question	PIMS
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Yes
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer Questions 37 a) - e) and describe your organization's policies/procedures for receiving and handling access requests below. Where NO, proceed to Question 38.	
a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.	Partially
b) Do you provide access within a reasonable timeframe following an individual's request for access? If YES, please describe.	Yes
c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.	Yes
d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g., email, same language, etc.)?	Partially
e) Do you charge a fee for providing access? If YES, describe below what the fee is based on and how you ensure that the fee is not excessive.	No
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended, and/or deleted? Describe your organization's policies/procedures in this regard below and answer Questions 38 a) - e).	
a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.	Yes
b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?	Yes
c) Do you make such corrections or deletions within a reasonable timeframe following an individual's request for correction or deletion?	Yes
d) Do you provide a copy of the corrected personal information or provide confirmation that the data has been corrected or deleted to the individual?	Yes
e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	Yes

[8] Accountability

The GCBPR's program requirements on accountability require organizations to be held accountable for complying with measures to implement the Privacy Principles.

PIMS also stipulates requirements for privacy policies, roles, responsibilities, authorities, communication, resources, competence, and awareness. The controls include determining and fulfilling obligations to PII principals, identifying legal basis, determining roles and responsibilities with joint PII controllers, and contracting with PII processors.

Regarding compliance with self-regulatory organization code and/or rules in Questions 39 and 46, Under "understanding the organization and its context," PIMS requires an organization to determine the internal and external issues that affect its purpose and its ability to achieve the intended outcomes of its PIMS. However, because there is no reference to the self-regulatory organization code and/or rules, it is assessed and marked "Partially".

For the complaint receipt, investigation, and response in Question 41 of the GCBPR program requirements and explanation of remedial action relating to complaints in Question 43, there are controls in PIMS for the handling of objections and requests, but there is no clear reference to an investigation as in Question 41. While the concept of response to requests is indicated in Question 43, there is no reference to an explanation of remedial action, and therefore, they are marked "Partially".

For Question 44, regarding privacy policies and procedures training, including how to respond to privacy-related complaints, while appropriate training is included in the requirements, there is no specific mention of the content of response to complaints, so it is assessed as "Partially".

Question 47 includes requiring personal information processors and others to abide by Global CBPR privacy policies and practices, seeking similar privacy practices, and being Global-CBPR-certified in their jurisdiction, which are unique to GCBPR and are therefore marked "No"

Question 48 concerns requiring personal information processors and others to submit self-assessments to confirm compliance with contracts, and Question 49 is regarding conducting checks and monitoring of personal information processors, etc. PIMS states that, in the contract with a PII processor, it is desirable for the business partner to submit appropriate information—including audit results in some cases—so as to demonstrate compliance with its obligations. However, because there are no further references to this matter, the assessment is marked "Partially".

Table 14 Comparison with GCBPR program requirements for accountability

Question	PIMS
39. What measures does your organization take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe below.	
- Internal guidelines or policies (if applicable, describe how implemented)	Yes
- Contracts	Yes
- Compliance with applicable industry or sector laws and regulations	Yes
- Compliance with self-regulatory organization code and/or rules	Partially
- Other	No
40. Has your organization appointed an individual(s) to be responsible for your organization's overall compliance with the Global CBPR Privacy Principles?	Yes
41. Does your organization have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Partially
42. Does your organization have procedures in place to ensure individuals receive a timely response to their complaints?	Yes
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	Partially

Question	PIMS
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Partially
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Yes
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?	
- Internal guidelines or policies	Yes
- Contracts	Yes
- Compliance with applicable industry or sector laws and regulations	Yes
- Compliance with self-regulatory organization code and/or rules	Partially
- Other (describe)	
47. Do these mechanisms generally require that personal information processors, agents, contractors or other service providers:	
- Abide by your Global CBPR-compliant privacy policies and practices as stated in your privacy statement?	No
- Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your privacy statement?	No
- Follow instructions provided by you relating to the manner in which your personal information must be handled?	Yes
- Impose restrictions on subcontracting unless with your consent?	Yes
- Be Global CBPR-certified by a Forum-recognized accountability agent in their jurisdiction?	No
- Other (describe)	No
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	Partially
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	Partially
50. Do you disclose personal information to other personal information controllers in situations where due diligence and mechanisms to ensure compliance with the Global CBPR System by the recipient as described above is impractical or impossible?	Partially

(6) Comparison with the requirements of the Global PRP program

The outcomes of the comparison with the requirements of the Global PRP program are shown below. Program requirements having equivalents are marked "Yes", "No" if there are none, and " Partially" if there are similar requirements but not considered equivalent. In addition, where a program requirement is broken down into options, items that are not treated as comparison targets—such as the leading question—are marked with a slash.

[1] Security safeguards

The Global PRP sets forth requirements for eight security safeguards to be met.

PIMS also specifies information security controls that require risk assessments and implementation of risk responses based on the results.

For Question 4 regarding detecting, preventing, and responding to security failures, PIMS includes references to fraudulent activity detection through the collection and analysis of logs and is therefore marked "Yes". However, there are no monitoring activities, such as those in ISMS, or controls for acquiring vulnerability information and detecting malware.

Regarding the test for the effectiveness of safeguards in Question 5, PIMS specifies the establishment and application of rules for development that consider the security of software and systems related to PII processing. However, security tests for development and acceptance are not included as a control and are thus evaluated as "Partially".

Table 15 Comparison of Global PRP program requirements for security safeguards

Question	PIMS
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	Yes
2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	Yes
3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.	Yes
4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	Yes
5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.	Partially
6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?	Yes
7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	Yes
8. Does your organization use third-party certifications or other risk assessments? Please describe.	Yes

[2] Accountability measures

The Global PRP sets forth the requirements for ten accountability measures to be met.

The PIMS also stipulates requirements for roles, responsibilities, authorities, resources, competence, and awareness. The controls include the agreement of the business partners, processing only at the business partners' direction, compliance with the obligations to PII principals, return, transfer, disposal of PII, notification of disclosure requests, and the disclosure of and engagement with subcontractors.

Question 13 relates to the procedures for forwarding complaints from the processor to the controller and the procedures for processing the controller's instructions. Although the control makes

it desirable for the processor to provide a means for the controller to comply with the obligations to PII principals, there are no more specific references from the same perspective as Question 13 and is therefore marked "Partially".

Question 17 c) requires the subprocessor to obtain Global PRP, which is unique to Global PRP and is therefore marked as "No"

Question 17 d) concerns requiring subprocessors to submit self-assessments to confirm compliance with the contract, etc., and Question 17 e) is concerning the inspection and audit of the personal information processors, etc., the control requires that the contracted party handling PII processing does so according to the contract. It also makes it desirable for business partners to submit appropriate information, including an audit in some cases, to verify compliance with their obligations. However, the control has no further reference to it and is therefore marked "Partially".

Question 18 refers to employee training as a requirement, and it is marked "Partially" because PIMS does not specify whether or not to provide training for "related client instructions."

Table 16 Comparison of Global PRP program requirements for accountability measures

Question	PIMS
9. Does your organization limit its processing of personal information to the purposes specified by the controller?	Yes
10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?	Yes
11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.	Yes
12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the Global PRP System?	Yes
13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	Partially
14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?	Yes
15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?	Yes
16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.	Yes
17. Does the mechanism referred to above generally require that subprocessors:	
a) Follow instructions provided by your organization relating to the manner in which personal information must be handled?	Yes
b) Impose restrictions on further subprocessing?	Yes
c) Be Global PRP-certified by a Forum-recognized Accountability Agent in their jurisdiction?	No

Question	PIMS
d) Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If YES, describe.	Partially
e) Allow your organization to carry out regular spot checking or other monitoring activities? If YES, describe.	Partially
f) Other (describe)	No
18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.	Partially

[3] Analysis of comparison outcomes

The following table summarizes the number of questions and the alignment rate for each of the eight principles of the Global CBPR: notice, collection limitation, use of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability, and for security safeguards and accountability measures of the Global PRP. The alignment rate was calculated by setting values of 1 for "Yes", 0.5 for "Partially", and 0 for "No"

The Global CBPR program requirements for notice, collection limitation, use of personal information, and integrity of personal information showed high alignment rates. By contrast, the alignment rate was below 100% for choice, security safeguards, access and correction, and accountability program requirements of the Global CBPR, and the Global PRP program requirements for security safeguards and accountability measures. Some controls in the program requirements of the Global CBPR, such as affordable measures, requesting personal identification in interactions, provisions for interactive formats, and investigation into complaints, are not specified at the same level of granularity as PIMS controls. Some security safeguards included in ISMS controls, such as physical entry/exit, antimalware, and vulnerability information collection, are not included in PIMS controls and therefore could not be judged as sufficiently aligned. Additionally, for the management of so-called contracted parties (management of processors in the case of Global CBPR and subprocessors with Global PRP), submitting self-assessments and conducting audits and inspections are required, and while PIMS has controls that conceptually correspond to these matters, they are not stated with sufficient clarity

Table 17 Alignment rates between Global CBPR/Global PRP and PIMS program requirements

Classification	Principle	No. of questions	No. of Yes	No. of Partially	No	Alignment rate	Observations
Global CBPR	Notice	10	10	0	0	100%	
	Collection limitation	5	5	0	0	100%	
	Uses of personal information	10	10	0	0	100%	
	Choice	7	6	1	0	93%	PIMS does not clearly address whether the choices offered are affordable.
	Integrity of personal information	5	5	0	0	100%	
	Security safeguards	15	10	5	0	83%	Some specific security-related controls were not sufficiently indicated by PIMS.
	Access and correction	11	8	2	1	82%	Specific controls, such as personal identification and interactive formats, were not indicated by PIMS at the same level of granularity.
	Accountability	22	12	7	3	70%	Specific grievance and training controls were not presented at the same granular level as PIMS. The queries specific to GCBPR and Global PRP did not align. In contracts with processors, some items, such as submitting self-assessments and conducting audits/inspections, were not clearly indicated in PIMS.
Global PRP	Security safeguards	8	7	1	0	94%	Some specific security-related controls were not sufficiently indicated by PIMS.
	Accountability measures	14	9	4	1	79%	In contracts with the subprocessors, some items, such as submitting self-assessments and conducting audits/inspections, were not clearly indicated in PIMS.

(7) Analysis of the strengths and benefits of GCBPR compared to other systems

Based on the above, more detailed strengths and benefits of GCBPR compared to other systems were analyzed, while also using the 2024 mapping survey, from the perspective of each of the following.

[1] Characteristics of the system overviews

Because GCBPR is aimed specifically at protecting personal information transferred across borders, its assessment scope is clearer than that of other similar certification systems.

While other certification systems are based on ISO/IEC international standards or Japanese Industrial Standards, GCBPR has developed its own Privacy Principles, frameworks, program requirements, and related materials with the participation of government bodies in the GCBPR Forum. Whether the applicant organization is a controller, processor, or both, their roles and responsibilities are individually defined and certified under the scheme, which is another unique feature of this certification system.

In addition, a distinctive framework for the GCBPR is the Global CAPE (Global Cooperation Arrangement for Privacy Enforcement). The Global CAPE is a practical multilateral framework through which privacy enforcement authorities (PEAs) cooperate on cross-border data protection and privacy enforcement. It does so by establishing arrangements under which PEAs can voluntarily share information and request and provide assistance in specified ways. By facilitating cooperation among PEAs, the Global CAPE provides the basis for trusted and accountable cross-border flows of personal information under the Global CBPR and Global PRP Systems.

It is also worth mentioning that a robust dispute resolution mechanism exists. GCBPR AAs handle complaints jointly with the government bodies of their own jurisdiction, and this function of the system serves to earn the trust of the individuals who provide their personal information.

Once a year, the system collects statistical data and case examples on the handling of complaints from each country's AAs and shares them among member countries. This not only contributes to the overall high reliability of the system but also promotes the improvement of assessment capabilities and standardization by the assessment bodies of each country. This is an essential mechanism for private bodies in different jurisdictions to function effectively as AAs, serving as an important self-regulatory mechanism (some countries/regions have governmental bodies serving as AAs).

Regarding ISMS, PIMS, etc., the International Accreditation Forum, Inc. (IAF) is an international body made up of accreditation bodies, associations of certification bodies, and national industry associations engaged in conformity assessment activities, such as for management systems, products, and personnel. It aims to develop a globally consistent conformity assessment scheme and reduce risks by ensuring the reliability of accredited certifications.[22]

[2] Certification unit

Since ISMS and ISMS-PIMS certifications are provided on an organizational basis, it is reasonable and advantageous for business operators to appropriately determine the scope of their management systems in accordance with the actual state of utilization. However, since certification must be obtained by each business and division, the system cannot be centralized or unified by an organization, and it may be more costly than GCBPR, which can be obtained at the individual company level, as multiple divisions incur certification costs. Additionally, when ISMS or ISMS-PIMS certified organizations consider applying for GCBPR, they must be aware of the need for

[22] ISMS-AC website “ISMS conformity assessment scheme” brochure https://isms.jp/doc/ismspamph.pdf

additional for each certification unit to accommodate changes in the assessment scope or consolidate the status of applications internally.

[3] Certification period[23]

The scheme for GCBPR is to resubmit the application each year (with monitoring conducted six months later). The period is every three years for ISMS and ISMS-PIMS, but because surveillance reviews are conducted within the certification period, it is the same in terms of a review each year. However, the scope of the review is narrower than that of the initial assessment or recertification review. The PrivacyMark is a system in which renewal assessment is conducted every two years, and the scope of assessment does not cover all business operations.

Opinions are divided regarding certification periods, and applicant organizations undeniably shoulder a heavy burden in terms of operations and management. However, the fact that a third party annually reviews all the operations enhances the reliability of the organization, which can be regarded as a strength.

[4] Certification costs

GCBPR calculates review fees on an estimate basis, taking into account the number of business operations involving cross-border data transfers subject to evaluation, data flow complexity, and number of transfer destinations (contracted parties, countries/regions to which data are transferred, etc.).

The PrivacyMark has fixed rates as review fees that are solely determined by the scale of the business operator and whether the certification is new or a renewal.

As with CBPR, ISMS and PIMS use variable fees based on estimates because man-days and costs vary according to the scope, locations, and number of personnel of the organization being assessed. Although limited, international standards are provided for determining audit man-days under ISO, and the requirements for certification bodies only specify the minimum number of audit man-days required. Therefore, when a request for review is filed under the same conditions, the fee will vary depending on the assessment body.

[23] Because GCBPR is not a renewal-based system, there is no renewal period but rather a certification period.

Table 18 (Reference) Comparison of GCBPR system overviews and existing certification systems

	Item	GCBPR	PrivacyMark	ISMS	ISMS-CLS[24]	ISMS-PIMS	ISMAP/LIU[25]	27018[26]
1	Managed object	Cross-border personal data	Personal information	Information assets	Cloud	Personal information	Cloud	Cloud Personal information
2	Objectives and managed objects	Protection of personal information transferred across borders	Protection and use of personal information (all personal information handled in business)	Proper management of information assets	Management specific the provision and use of cloud services	Appropriate management of personally identifiable information (PII)	Security standards for government information systems	Protection of PII on the public cloud
3	Standard, etc.	GCBPR requirements	The PrivacyMark operational guidelines	27001 requirements	27017 requirements	27701 requirements	ISMAP control criteria	27018 code of practice[27]
4	Conformity	Must meet all requirements	Must meet all requirements	Must meet all requirements and controls	-	Must meet all requirements (controls may be added or excluded)	-	-
5	Year started[28]	2025	1998	2002	2016	2021	2020	-
6	Certification unit	Corporation (Japan) (Corporation as a unit after identifying the business covered)	Corporation (Japan) (Exceptions for incorporated educational institutions and medical corporations)	Organizational (The scope can be specified)	ISMS scope or a portion of it	Organizational (The scope can be specified)	Cloud services	-
7	Recertification period	1 year (monitoring after six months)	2 years	3 years (annual reviews conducted)	3 years (annual reviews conducted)	3 years (annual reviews conducted)	1 year and 4 months	-
8	Number of certifications obtained (in Japan)	4	17707	8009	615	68	77/1	-

[24] An add-on certification requiring prior ISMS certification. It is a system to verify the implementation of security safeguards against the risks inherent in cloud services, based on the international standard ISO/IEC 27017 as the control standard.

[25] ISMAP is a security assessment system for government information systems. It is an assessment standard established by METI as certification for SaaS providers that handle services with low security risks.

[26] ISO/IEC 27018 is an international standard for protecting personal information managed by cloud service providers on the public cloud. It is a standard for organizations that operate cloud services (PII controllers).

[27] The certification standards established by the assessment body.

[28] The year started does not refer to the year in which the system commenced, but it is the year in which certification began in Japan.

	Item	GCBPR	PrivacyMark	ISMS	ISMS-CLS[24]	ISMS-PIMS	ISMAP/LIU[25]	27018[26]
9	Number of assessment bodies (in Japan)	1	20	27	18	5	4	-
10	Review fees	Estimate	Fixed rate	Estimate	Estimate	-	-	-
11	Review method	Self-assessments of business operators are reviewed (document reviews, on-site assessment)	Review of the personal information protection management system (document reviews and on-site assessment)	Review of the information security management system (initial assessment: [1] first stage review and [2] second stage review)	Review of the privacy information management system (initial assessment: [1] first stage review and [2] second stage review)	-	-	-

[5] Program requirements perspective

In terms of program requirements, the alignment rate was generally high between GCBPR and PrivacyMark and PIMS, and even items with a low alignment had an alignment rate of 70% or higher. Alignment rates for requirements related to information security and contracted party management were low.

In comparing the individual certification systems, since ISMS is an information security management system targeting information assets, more specific controls have been established by ISMS for information security than by GCBPR, resulting in higher alignment rates. Although PIMS does not fully align with the Privacy Principles or specific program requirements, it covers all of them at the principle level. However, as with ISMS, PIMS is a management system certification and is fundamentally determined based on a risk assessment. The same can be said for the PrivacyMark as it is also a management system.

As a result, the controls for ISMS, PIMS, and PrivacyMark tended to have relatively abstract expressions, while GCBPR program requirements were found to be concrete and effective, which can be seen as a strength.

Table 19 (Reference) Comparison of CBPR program requirements with 2024 Research results for PrivacyMark and ISMS

Principle	2024 Research results		This research	Observations
	PrivacyMark	ISMS	PIMS	
Notice	100%	10%	100%	Both require the establishment of policies, but the ISMS does not include detailed requirements for the content of the notice.
Collection limitation	100%	0%	100%	The PrivacyMark and PIMS are 100% aligned. However, since ISMS does not necessarily include personal data, the degree of alignment is low, reflecting differences in purpose between the certification systems.
Uses of personal information	100%	0%	100%	The PrivacyMark and PIMS are 100% aligned. However, since ISMS does not necessarily include personal data, the degree of alignment is low, reflecting differences in purpose between the certification systems.
Choice	100%	0%	93%	Although PrivacyMark and PIMS have a high degree of alignment, ISMS does not necessarily include personal data; thus, the degree of alignment is low, reflecting differences in purpose between the certification systems.
Integrity of personal information	100%	100%	100%	PrivacyMark, ISMS, and PIMS are aligned, indicating that data integrity is a critical requirement for these systems.
Security safeguards	83.3%	100%	83%	There was 100% alignment with ISMS, but some controls in PrivacyMark and PIMS were not sufficiently described.
Access and correction	100%	0%	82%	Although PrivacyMark and PIMS have a high degree of alignment, ISMS does not necessarily include personal data, so they are not aligned, reflecting differences in purpose between the certification systems.
Accountability	91.3%	91.3%	70%	The PrivacyMark and ISMS are highly aligned, but PIMS has a lower alignment rate than the other two due to the impact of the revised interpretation of survey items.

[6] Supporting evidence

In Japan, GCBPR applicant organizations must fill out the Global Cross-border Privacy Rules (CBPR) System Intake Questionnaire and the Additional Questionnaire showing compliance with the certification standards of the respective AA, conduct self-assessments, and submit supporting evidence for the assessment results. The GCBPR will review the documents on the basis of the supporting evidence for the assessment results in each questionnaire.

Examples of supporting evidence to be prepared by GCBPR applicant organizations in the form of policies and regulations and records were compared with material required to be documented or recorded according to the PIMS standard and controls for PII controllers. Documentation of required equivalent content is marked with "Yes". When the required documentation is not equivalent but similar, it is marked "Partially". Otherwise, the notation "No" is applied.

The following table shows the results of comparing examples of supporting evidence for the self-assessment results (policies and regulations) required in GCBPR review with the PIMS standard and controls.

Table 20 Examples of supporting evidence (policies and regulations) assumed in GCBPR review

	Examples of supporting evidence (policies and regulations) assumed in GCBPR review	PIMS
1	Privacy policies (privacy statements, personal information protection policies, etc.)	Yes
2	Regulations regarding procedures for identifying personal information	Partially
3	Regulations for the identification, reference, and maintenance of laws and regulations, national guidelines, and other codes	Yes
4	Regulations for procedures to identify, analyze, and take measures against risks related to personal information	Yes
5	Regulations for authority and responsibility for protecting personal information in each division of the business operator	No
6	Regulations for response to emergency situations (leakage, loss or damage, etc. of personal information)	Yes
7	Regulations for the acquisition, use, and provision of personal information	Yes
8	Regulations for the proper management of personal information (rules regarding contracted parties, employee management, security control, etc.)	Partially
9	Regulations concerning training	Yes

1, 3, 4, 6, 7, and 9 have been marked "Yes". The standard and controls for PII controllers in PIMS have references to documentation, such as privacy policies, legal basis related to PII processing, privacy risk assessment and risk response processes, information security incident response procedures, consent process, competence, etc.

Regarding "2. Regulations regarding procedures for identifying personal information," PIMS requires documentation for identifying purposes but does not specifically require identifying personal information. However, item 2 was classified as "Partially" because controls are stipulated for records related to PII processing.

Regarding "5. Regulations for authority and responsibility for protecting personal information in each division of the business operator," although the allocation of responsibilities and authorities is required in PIMS, documentation is not clearly required, and therefore, this item is marked "No"

Regarding "8. Regulations for the proper management of personal information (rules regarding contracted parties, employee management, security control, etc.)," the information security controls cover only part of the requirements. In addition, contracts with PII processors and confidentiality or non-disclosure agreements for employee management are assumed. This item is marked "Partially", taking into account that the object of comparison in this table is regulations rather than contracts.

The following table shows the results of comparing examples of supporting evidence for the self-assessment results (records) required in GCBPR review with the PIMS standard and controls.

Table 21 Examples of supporting evidence (records) assumed in GCBPR review

	Examples of supporting evidence (records) assumed in GCBPR review	PIMS
1	Organization chart and GCBPR structure	No
2	System configuration (system configuration diagrams, network diagrams, and other system specification documents)	No
3	Security policy (basic information security policy, etc.)	Yes
4	List of risk analysis and measures to be taken for each risk	Yes
5	Document provided to individuals upon personal information collection	Yes
6	Ledger for identifying and managing personal information	Yes
7	List of contracted parties and data recipients	No
8	Records of evaluation and selection of contracted parties and data recipients	No
9	Contracts with the contracted parties and data recipients	Yes

3, 4, 5, 6, and 9 have been marked "Yes". PIMS requires information security programs, including a set of policies for information security, documentation of the privacy risk assessment outcomes and response results, maintenance of records related to PII processing, and obtaining and documenting consent. In PIMS, contracts with PII processors and joint PII controllers are assumed.

For 1, 2, 7, and 8, no documentation was explicitly required in PIMS, and these items are therefore marked "No" PII handled between an organization and its contracted parties and data recipients is verified based on the relevant contracts, and therefore no documentation of supporting evidence to confirm operations, such as the organizational structure, system configuration, the status of contracted parties and data recipients, and selection criteria, is required.

From the above, it can be seen that several examples of supporting evidence required for GCBPR review are consistent with those required for documentation and recording in PIMS review.[29]

<List of References>

- GLOBAL CROSS-BORDER PRIVACY RULES SYSTEM (CBPR) PROGRAM REQUIREMENTS MAP
- GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEM PROGRAM REQUIREMENTS MAP
- ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

[29] It does not refer to all supporting evidence. There was an alignment between GCBPR and PIMS in several supporting evidence examples.

2.4. Detailed Analysis of the Corporate Certification Process and Study into Improving Its Efficiency

(1) Survey objective

Based on the results of the comparative analyses of Subsection 2.3. in this research, 2024 mapping survey, and AA questionnaire in 2024,[30] measures were considered to streamline the corporate certification process at AAs.

(2) Survey period

From Thursday, October 23, 2025 to Wednesday, November 19, 2025

(3) Survey targets

Based on the results of the comparative analyses of Subsection 2.3. in this research, the 2024 mapping survey, and the 2024 AA questionnaire, eight AAs accredited by the GCBPR Forum were asked to respond to the questionnaire in order to collect information that would contribute to a detailed analysis of the certification process and consideration of its efficiency. A total of nine organizations, including JIPDEC, were included in the survey.

Table 22 Organizations taking part in the questionnaire

Accessed on November 30, 2025

	Name of the Organization	Overview		
		Management entity	Year certification began	Number of certifications[31] CBPR/PRP/Both (Number of certified organizations)
1	TrustArc (U.S.)	Private sector	2013	32/25/6 (51)
2	Schellman (U.S.)	Private sector	2019	5/12/3 (14)
3	NCC Group (U.S.)	Private sector	2020	5/6/5 (6)
4	BBB National Program (U.S.)	Private sector (Non-profit)	2021	7/7/2 (12)
5	VeraSafe (U.S.)	Private sector	2025	- / -
6	IMDA (Singapore)	Government body	2019	12/6/4 (14)
7	KISA (Republic of Korea)	Government-commissioned	2019	12/ - (12)
8	III (Chinese Taipei)	Government body	2021	1/ - (1)
9	JIPDEC (Japan)	Private sector (Non-profit)	2016	4/ - (4)
Total number of certified organizations				114[32]

[30] Refer to the 2024 Research Report, Chapter 2: Activities for Disseminating CBPR, 2.1.3 Questionnaire for AAs (pp. 49-53).

[31] GCBPR Forum https://www.globalcbpr.org/privacy-certifications/directory/
The total number of certifications differs from the total number of certified organizations because a business operator with both certifications is counted once for Global CBPR and Global PRP each. The number of certified organizations is shown in parentheses.

[32] 114 companies is the total number of certified organizations.

(4) Survey items

A total of five questions were established in three categories, focusing on the review process and process items being prioritized.

<Questionnaire items>

Assessment Questionnaire Response Form

Questions Regarding efficiency in the review process
These Questions focus on the efficiency of the review process. For Q1 through Q3, please provide as much detail as possible regarding the review procedures.

Question 1
Please describe the specific steps of the review process, along with the man-days and number reviewers, using the format below. *Sample (next page: Process by JIPDEC)

Question 2
Please mark * in the critical process item within the review process and explain why you consider them important.

Reason:

Question 3
Please explain the basis for determining the number of Assessors (e.g., data volume, company requests, number of operations under evaluation).

Question 4
Are there forms or checklists used by Assessors during the audit process? (Y/N) If "Yes", please list them below by audit stage.

Process Stage	Form Name and Purpose
Document Review	1. (Purpose/Description)
	2. (Purpose/Explanation)
Hearing	3. (Purpose/Description)
Report	4. (Purpose/Description)

Question 5

Please tell us about the review fees.

(5) Survey method

The questionnaire for AAs was conducted with the consent of the organizations surveyed, the GCBPR Forum, and the Personal Information Protection Commission (the commissioning organization), which is the competent authority for the GCBPR. Since the questionnaire included

confirmation of the detailed process and man-days required for the certification process, an explanation of the purpose of the questionnaire survey, including improving the efficiency of the certification process, was provided when the questionnaire form was sent out to encourage cooperation in the survey.

(6) Results for each of the questions

[1] Please describe the specific steps of the review process, along with the man-days and number reviewers, using the format below. (Q1)

- **The specific review process**

In the 2024 Research, there was no significant difference in the review process among the AAs. It was a process in which document reviews and reviews of those documents were conducted multiple times, assessment reports were prepared, applicants were asked to make corrections, and certification was granted upon completion.

In this research, a detailed investigation of the common review process revealed that AAs conducted reviews according to their own process. The major difference was whether or not on-site assessments were being carried out, with six organizations doing so.

The review process of each of the AAs was evaluated using common items based on responses, except for those independently established.

Table 23 Items for evaluating the review process

Review process	Contents of the review
Document review	The 50-question conformity assessment
	Confirmation of deficiencies and corrective actions
	Secondary review and final assessment
On-site assessment	On-site evaluation
Report	Report preparation and review
	Preparation and review of report for corrective actions
Assessment of the appropriateness of the review	Review of the report
	Deliberation on the grant of certification
Certification granted	Notification of review results and issuance of certificate (accreditation)

The detailed evaluation results for each of the AAs are described in the supplementary material (Summary of AA questionnaire_published version 1).

- **Man-days**

It was shown that man-days are relatively few for AAs using online platforms.[33] It could also be seen that man-days for AAs conducting on-site assessments tended to be generally greater than those of AAs that do not.

Also, some AAs that conduct on-site assessments were found to have fewer man-days as a result of combining them with the use of online platforms.

[33] A web-based application system created and offered by the U.S. Department of Commerce, or platforms that AAs developed independently.

The total number of man-days for each of the AAs is as follows. For AAs that responded with number of hours, calculations are based on 8 hours per person per day. Man-days before and after the review process are excluded.

Table 24 Man-days

Assessment body	Total man-days
A	No response
B	13.5-24.5 man-days
C	Not disclosed
D	1.3-1.7 man-days
E	Small-scale: 7-11 man-days Large-scale: 12.3 - 18.3 man-days
F	4.5-20.5 man-days
G	132 man-days
H	22-36 man-days
I	44 man-days

*Assessment bodies 1-9 in Table 22 and A-I in Table 25 are listed in no particular order and do not correspond to one another (the same applies hereafter).

Table 25 Comparison with the use of online platforms

	A	B	C	D	E	F	G	H	I
Man-days	-	High	-	Low	Low	Low	High	High	High
Online	Yes	No	Yes	Yes	Yes	Yes	No	No	No

Table 26 Comparison with the conducting of on-site assessments

	A	B	C	D	E	F	G	H	I
Man-days	-	High	-	Low	Low	Low	High	High	High
On-site assessment	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes

- **Period**

The review period was as shown in Table 28, ranging from 2.25 to 6 months depending on the organization. The results of the AA questionnaire showed no correlation between the review period and any of the following: man-days, use of an online platform, or whether an on-site assessment was conducted.

The response by one AA included the monitoring process in addition to the initial certification, with a review period of nine months, including 2.25 man-days for monitoring.

Table 27 Review period

Assessment body	Period
A	3 - 6 months
B	3.3 - 4.3 months
C	2.3 - 4 months
D	No response
E	3.7 - 4.7 months
F	No response
G	4 months
H	4 months (plus varying on-site assessment period)
I	3.5 - 4 months

- **Number of assessors per company**

The number of assessors involved in each review process per company ranged from 1 to 4. Of the nine organizations, excluding one for which the number was unknown, seven AAs listed the minimum number of assessors as one. In addition, five organizations listed 3 assessors as the maximum number, accounting for a majority of the AAs. There were many that provided no response or responded that the number of assessors varies. The basis for determining the number of assessors will be discussed later in Q3.

Table 28 Number of assessors per company

Assessment body	Number of assessors
A	Unknown
B	1-3
C	1-3
D	1-2
E	1-3
F	1-2
G	1-4
H	1-2
I	2-3

[2] Please mark * for the critical process items within the review process and explain why you consider them important (Q2).

Most AAs responded that the document review, 50-question conformity assessment, is a critical process item, and many responded that it was followed by document review: confirmation of deficiencies and corrective actions, and on-site assessment: on-site evaluation, as important process items.

Because the review process differed among the AAs that responded, they were evaluated in a standardized review process.

The breakdown of steps in the process that the AAs positioned as important is as follows.

- **Most important**

  Eight AAs position document review: 50-question conformity assessment as the most important step, with the main reason being that it is an assessment of compliance that forms the basis of the certification system and directly supports the reliability of the certification.

- **Important process items**

  Document review: The confirmation of deficiencies and corrective actions is an important process item for the six AAs, mainly because it is essential for identifying areas of non-compliance and deficiencies, and to address them prior to granting certification.

  On-site assessment: on-site evaluation was positioned as an important process item by four of the six AAs that are conducting them. The main reason cited was being able to ensure the integrity of certification by directly checking on-site the implementation of documented policies and procedures.

- **Other important process items**

  Several AAs identified document review: secondary review and final assessment; report: report preparation and review; and assessment of the appropriateness of the review: deliberation on the grant of certification, as important process items.

  In all cases, it was found that efforts were made to ensure the quality of certification and assurance by incorporating multiple perspectives into each review step and introducing the step of deliberation and evaluation of review results by another third party into the review process.

[3] Please explain the basis for determining the number of Assessors (e.g., data volume, company requests, number of operations under evaluation). (Q3)

Although the number of assessors per company is as shown above, most AAs point to the number of operations that handle personal data subject to evaluation, complexity of the systems and data flows, and the type of information (confidentiality), etc. as the basis. The number of assessors is also determined based on the volume of personal data and the number of locations subject to assessment.

The detailed basis for determining the number of assessors for each of the AAs is as follows.

Table 29 The basis for determining the number of assessors

Name of the Organization	The basis for determining the number of assessors
A	- Environmental complexity It is usually performed by two assessors, but there may be three when the functions are complicated, the volume of data flow is large, or additional confirmation is necessary due to deficiencies in the content.
B	- Assessment structure Two separate teams must conduct the assessment, one of which makes the certification decision. This is to ensure that certification decisions are based on a comprehensive review.
C	- Environmental complexity It depends primarily on the data volume and complexity of the applicant's operations. Organizations with multiple data flows, subsidiaries, or activities across several jurisdictions typically require additional assessors to ensure a thorough and efficient review. - Team composition It also depends on the proficiency and experience of the assigned staff. If team members are inexperienced or unfamiliar with the GCBPR review process, more experienced assessors are paired with them to provide supervision and quality assurance. This approach balances workloads, facilitates learning, and maintains consistency of the certification results.
D	- Defining the scope of operations to be evaluated It is conducted on a man-month basis. Examples: [1] Simple scope (when security and privacy measures are based on a decentralized approach): One assessor for three weeks [2] Where centralized decision making and application of controls across multiple products/services is required: Two assessors for two weeks - Important considerations The number of operations subject to evaluation, the size of the target systems, and the number of privacy notices to be reviewed are more important than the data volume. - Man-days and number of assessors It depends on the complexity of the organization's scope of assessment, whether it is centralized or decentralized, whether it reviews external service providers, internal operations/ employee data, or a combination of both.

Name of the Organization	The basis for determining the number of assessors
E	- Environmental complexity Organizations with multiple business units, diverse data flows, or complex international operations typically need more days for assessment to adequately cover all aspects. - Data volume and confidentiality Increased volume of personal data processing and more sensitive data categories (health records, financial information, etc.) may require additional assessment days to ensure thorough assessment of privacy management and risk mitigation measures. - Size and structure of the organization Larger organizations with multiple subsidiaries, joint ventures, or complex corporate structures will require more assessment days to properly evaluate privacy practices in all organizations seeking certification.
F	- Scope of the assessment The number of systems, applications, and operations to be assessed. - Risk assessment Determined based on the volume and confidentiality of personal data to be handled and whether the organization functions as a controller or processor. - Environmental complexity The higher the complexity or data volume, the more testing and assessors are required. - Client requests or scope definition Workload increases for assessment of organizations that have chosen to include additional systems and services. - Internal scheduling and structural safeguards Operations are managed by the operations management team and approved by the operations manager to ensure appropriate staffing and avoid conflicts of interest.
G	- Environmental complexity The number of personal data handlers, personal data volume, number of information systems, and number of subcontractors (e.g., data processors) of the applicant organization have been considered.
H	- Data volume /complexity Very large user databases, multiple data categories requiring parallel sampling. - Number of operations to be assessed Multiple, distinct processing operations or business lines. - Sites/ jurisdictions Processing and transfers involving multiple sites and jurisdictions. - Risk analysis by sector More in-depth technical coverage may be required for the financial and medical sectors.

Name of the Organization	The basis for determining the number of assessors
I	- Number of operations with cross-border personal data transfers - Data volume - Number of transfer destination countries/regions - Number of contracted parties - Complexity of the theoretical design of systems handling data and complexity of data flows - Complexity of the basis for personal data transfer (under domestic laws)

[4] Are there forms or checklists used by Assessors during the review process? (Q4)

This research revealed that all AAs have forms and checklists for use in the review process.

Each AA has prepared its own forms, as follows.

Table 30 Forms and checklists

Name of the Organization	Forms and checklists
A	- Multiple forms, including reports, tests, and report review workflows, are used across the company. - Extensive checklists are used particularly for the quality assurance (QA) and reporting processes, with comprehensive validation in terms of testing, reporting and certification.
B	- Report formats are in place for use at each stage of document review, interview, and on-site assessment. - A mechanism has been developed to systematically collate the documents submitted by the applicant against the specific criteria required by the CBPR Framework, using the Global CBPR System Program Requirements Map or an internal checklist based on it.
C	- Cheat sheets and common templates are in place for use at each stage of document review, interview, and reporting. - At the document review stage, a cheat sheet is used to support documentation related to the questions and includes a comprehensive list of documents required to establish sufficient evidence. - At the interview stage, common templates are used for supporting evidence that is lacking and for discussion points with the business operator and issues outstanding. - At the reporting stage, a research report is prepared and a detailed description of the business operator's compliance with all requirements is provided.
D	- Evaluation is conducted on the platform and digital evaluation tools are utilized.

Name of the Organization	Forms and checklists
E	- Different forms are used at multiple stages. - At the document review stage, a CBPR evaluation worksheet, a summary of evidence checklist, and the official intake CBPR questionnaire are used to ensure complete documentation and evidence control at each stage. - At the interview stage, the kickoff meeting agenda template is used to structure initial consultations with applicants. - At the reporting stage, a template is used to summarize compliance results. - A project management app is used to monitor the progress of submissions and verify that all required materials have been uploaded.
F	- Multiple forms are used during the questionnaire and document review stages. - Specifically, a total of seven formats have been prepared, including Form 1-1 (application), Form 1-2 (preliminary survey questionnaire), Global CBPR/PRP program requirements checklists, scope and mapping checklist, review/test work records, quality assurance (QA) review checklist, certificate set, and certification contract. * The forms are intellectual property, and detailed disclosure is restricted.
G	- The content of the self-assessment form that business operators submit are reviewed by an assessment body that are appointed by the AA. The AA reviews and approves reports, etc. prepared by the assessment body.
H	- Several forms are used at each stage of the deliberation process, including document review, preliminary review, on-site assessment, and certification granting. - Specifically, Form 1 (application), Form 2 (intake questionnaire), Form 3 (detailed specification for privacy control systems), Form 4 (checklist and non-conformity report), and Form 5 (audit report) have been prepared. - Form 3 requires the input of detailed information, such as the status of cross-border data transfers, handling of statutory certification schemes, and personal data processing flows.
I	- Five types of forms have been prepared for various stages, from document review to certification review meeting. - Specifically, Form A (inspection list), Form B1 (list of transfer destinations), and Form B2 (transfer destination management status sheet) are used in the document review stage to confirm whether the content of the application from the business operator is appropriate. - Form C (list of issues identified) is available for checking or pointing out issues regarding Forms A, B1, and B2 during the review stage. - After all reviews have been completed, the review results are compiled using Form D (review results report).

The forms and checklists used by AAs are positioned as essential mechanisms for ensuring review quality and maintaining transparency.

[5] Please tell us about the review fees. (Q5)

Other than KISA, which is commissioned by the government and is free of charge (temporarily being operated with government funds), responses ranged between US$3,600 and US$65,445 (as of the survey period from October 23 to November 19, 2025). However, review fees for most AAs are set based on the size, revenue, and business type of the applicant organization, and some AAs have not set an upper limit.

The detailed review fees for each of the AAs are as follows.

Table 31 Review fees

Assessment body	Review fees
A	- Global PRP: US$8,000 and above - Global CBPR: US$18,000 and above
B	- Base fee of US$10,000 and above
C	- Small-scale/ mature business operators: US$24,210-US$38,220 (Discounted pricing US$16,925-US$26,625) - Large-scale/ complex/ initial: US$44,010-US$65,445 (Discounted pricing US$30,925-US$45,875)
D	US$3,800-US$15,000 *based on the size of applicant organization
E	US$3,600 and above (Certification application fee, US$900; document review fee, US$1,800; on-site assessment fee, US$900/man-day)
F	Free of charge, commissioned by a government body
G and H	Not disclosed

(7) Measures by AAs to streamline the certification process

Based on the above, the measures for streamlining the certification process were summarized from the following viewpoints in conjunction with Subsection 2.3. of this research, 2024 mapping survey, and AA questionnaire in 2024.

[1] Reduction in man-days in the review process

Most AAs responded that the document review: 50-question conformity assessment was one of the important process items. When comparing with other certification systems, it became clear that AAs shared the same view regarding the importance of appropriate assessments, in light of issues such as ensuring the quality and consistency of assessments by private assessment bodies and maintaining the credibility of the system.

If focus is placed on this step and a review process is developed based on the other findings, such as a shorter review period and a minimized number of assessors, this will lead to a reduction in overall CBPR man-days and could also enable a reduction in review fees, etc.

Furthermore, as it has become clear that AAs using an online platform require fewer man-days, investigation should continue into the impact of using online platforms in the review process and factors that can reduce man-days from both system and operational perspectives, in order to identify effective ways to reduce man-days in the review process.

Even if the system that the U.S. Department of Commerce can provide to AAs were to be used, it would need to comply with the laws and regulations of each country. Therefore, when introducing the system, it is necessary to keep in mind that considerable time and effort are required for preparation, such as development costs and resources.

The one-year GCBPR certification period is shorter than the three-year ISMS certification period, but ISMS conducts annual surveillance reviews over a three-year period. If the GCBPR can build an assessment mechanism that can assure certification quality, both the AA and the applicant organization may be able to eliminate part of the process and reduce operating costs.

[2] Incentive to obtain multiple certifications

In the interviews with companies in Subsection 2.2. of this research multiple business operators reporting that the burden was placed on operations after obtaining certification and several respondents pointed out that the labor and costs involved in operating the certification system were more significant than the review fees being made free of charge. Business operators who have actually obtained ISMS and currently have more than one certification said that although the databases and ledgers to be referenced are the same, the documents to be submitted for each certification need to be processed and formatted individually, incurring separate man-days.

GCBPR is a more recent certification than other third-party certifications, such as PrivacyMark and ISMS. If a mechanism could be established to simplify assessment for business operators that have already obtained other certifications, man-days for assessment can be reduced. Operating costs can also be lowered for business operators, which may lead to an increase in the number of organizations getting certified.

An AA indicated on the AA questionnaire that, in some instances, the fee may be lower when certification is provided together with other certifications. Such cases may also be true for other AAs, and further investigation should be conducted to determine not only whether the review fees can be lowered but also whether any part of the review process and document submissions can be omitted or simplified.

III. Recommendations on Public Relations and Outreach Activities

1. Objectives

The survey questionnaire and interviews in Chapter II clarified the current situation in which the GCBPR is not well understood or widely recognized and identified the types of information required by business operators and the priority target audience. These details are described later in Section 3. Points to Note During Public Relations and Outreach Activities.

Based on the findings of the research, this chapter identifies effective public relations activities to disseminate GCBPR and increase the number of jurisdictions and companies participating, and also suggests useful indicators.

2. Current Status and Issues of Public Relations and Outreach Activities

2.1. Status of Information Dissemination

[1] Websites

The most accurate and up-to-date information regarding GCBPR, including an overview of the GCBPR System and procedures required to submit an application, can be obtained on the website of the Global CBPR Forum, the organization operating GCBPR. Information on GCBPR from sources in Japan is available on the websites of the Personal Information Protection Commission and the Ministry of Economy, Trade and Industry, which are the competent authorities for GCBPR, as well as JIPDEC, the Japanese assessment body. As this information can be freely accessed by potential GCBPR applicant organizations at any time, it is a very useful source of information for both system administrators and applicants.

Other websites that currently disseminate information include those of certified organizations and consulting firms that support organizations in obtaining GCBPR certification.

[2] Seminars and symposia

Seminars and symposia promoting and raising GCBPR awareness, which were noted in the 2024 Research, are good opportunities to hear directly from system-related parties and certified organizations in person. They serve as a good means of communication, making the information easier to understand than text-based material, and provide valuable opportunities to clarify unclear points.

[3] Other

Common PR tools include brochures and leaflets, but the competent authorities or assessment bodies currently do not publish any.

2.2. Issues

Section 2.1 examined the current state of information dissemination, focusing on where and how GCBPR information can be obtained. This section identifies the issues currently being faced from the perspective of information providers and potential applicants in order to support effective public relations and outreach activities going forward. In evaluating accessibility, content, and clarity, if feedback obtained from business operators in the interview survey is reflected, it is marked "Yes"; if some measures are in place but are insufficient, then "Partially"; and if no measures are in place, it is marked "No".

(1) Websites

[1] GCBPR Forum

- Accessibility: Yes

Information on the Global CBPR and Global PRP systems is available on the homepage.

- Content: Partially

The website is designed such that necessary GCBPR information can be accessed from the menu bar at the top of the homepage, and forms can also be downloaded from the links. However, for business operators accessing the website for the first time, there is no detailed overview of the GCBPR system or the specific benefits that applicant organizations can gain.

- Clarity: Partially

Information is categorized in the menu at the top of the homepage, but evaluation is close to "No" and marked "Partially" because the pages contain information mainly presented in text form and are not designed to aid visual understanding. Those unfamiliar with GCBPR may have difficulty finding the necessary information from the menu titles.

[2] Competent authorities of the GCBPR (the Personal Information Protection Commission and the Ministry of Economy, Trade and Industry)

- Accessibility: "No"

It is difficult for business operators to obtain necessary information from ministry and agency websites because there are no links on the homepage, and searches with keywords "CBPR" and "GCBPR" on the homepage do not readily lead to the relevant pages.

- Content: Partially

Although it is possible to gain an understanding of international developments, the websites lack any uniqueness as a ministry or agency and merely provide press releases from the Global CBPR Forum (the organization that operates the system) in Japanese. Thus, the fact that the Japanese government supports an international certification system for cross-border personal data transfers is not properly conveyed. Material in English conveying the benefits of the system is available on the Personal Information Protection Commission website. However, the information primarily focuses on legal requirements, and handling of cross-border data under the Act on the Protection of Personal Information (APPI) and benefits of the GCBPR system are not easily understood unless they are presented clearly. The information is insufficient to meet the needs of companies accessing the site out of certification interest and is therefore marked "No".

- Clarity, etc.: "No"

There is no dedicated page for GCBPR, and it is difficult to gain an overall understanding of the system, as information is provided sporadically and unconnected. It is also difficult for business operators visiting these ministry and agency websites for the first time to learn about GCBPR because the information is mainly text-based.

[3] JIPDEC (Assessment body)

- Accessibility: Yes

A banner titled "CBPR certification" can be found under "Find by business" on the homepage, and one click will take users to the dedicated page for the system.

- Content: Partially

Application forms and practical information regarding certification standards and case examples of certified organizations are available on the website. However, links to the GCBPR Forum

press releases and competent authority press releases are provided, and the website is not structured to introduce the system's appeal and benefits from the assessment body's unique viewpoint.

- Clarity, etc.: Partially

A short video introducing the CBPR system is provided at the beginning of the dedicated page. Additionally, a link to a six-minute video is provided for business operators seeking to learn more, which shows the efforts being made to promote understanding of the system in a short period according to the objective. Meanwhile, application documents can be downloaded from the website, but if a video explaining the review process and providing a sample for filling in the documents is available, it may be easier to understand the process up to the application submission.

[4] Consulting firms

- Accessibility: "No"

A review of the websites of about three business operators out of the results from searches with keywords such as "CBPR consulting" showed that none had banners or dedicated pages for CBPR on their homepages.

- Content: Partially

Although it was possible to view press releases issued by the competent authorities and the assessment body, searches with the keyword "CBPR" on the homepage of these websites showed that only one business operator had created a dedicated page (as of the time this report was prepared).

- Clarity, etc.: Partially

The website of the one business operator that had created a dedicated page was primarily centered on text-based information, and no explanations from a unique viewpoint were found. Therefore, it is difficult to gain sufficient understanding from the information presented alone.

(2) Seminars and symposia

- Accessibility: "No"

Information on seminars and symposia is buried deep within the websites of the competent authorities, and the information provided depends on the organization being entrusted with the seminar or symposium. Therefore, as means of communication are limited to announcements on individual organizations' websites, the information is highly likely to not reach the target audience. A business operator that is very interested in participating in the event may find it difficult to find or access the information. In the past, event venues have been limited to Tokyo, Osaka, and Fukuoka. Business operators outside these regions are unable to participate because of difficulty accessing these locations.

- Operation and content: Partially

Although competent authorities have held seminars in the past, they have been isolated events with little continuity. The schedule for the next event remains uncertain, and there is no mechanism linking the seminars and symposia with the system's continuous understanding and follow-up. As with the issue noted in (1) Websites, the events offer very few instances of the system's appeal and benefits being presented from the respective viewpoints and positions.

- Clarity, etc.: Partially

Case examples of certified organizations were sometimes introduced, and expert panel discussions were also held. However, since the events mainly consisted of text-based materials and keynote speeches, the lecture-style format and the information presented during that time alone were insufficient in providing clarity.

2.3. Improvement Measures

Based on the current status and issues raised in Section 2.2, this section summarizes measures for improvement. Note that the GCBPR Forum website has been excluded as it cannot be directly improved.

(1) Websites

- Place GCBPR banners (competent authorities) on the homepage.
- Introduce the benefits of the system and an abundance of certification examples from the unique viewpoint of the competent authorities and assessment body.
- Clearly communicate that the system is intended for a wide range of entities, including large enterprises and small and medium-sized enterprises (SMEs), as well as legal and information security specialists and persons in charge in the relevant divisions.
- Consider ways to increase website access (in collaboration with social media and industry media).
- Design the website in a way that the information on the page is presented not only in text but also using illustrations, videos, and other content that supports visual understanding.
- Use search-linked advertising, etc. to approach those who actively seek information and drive traffic to the website. Specifically, when users search for keywords such as "cross-border transfer," "personal information overseas," "cloud service personal information protection," "GDPR compliance," "data protection for expansion into Asia," "overseas subsidiaries," and "overseas expansion," ads can be displayed to direct them to GCBPR information pages.

(2) Seminars and symposia

- Meetings should be held in person several times on a regular basis, not only in large cities but also in regional areas.
- Online meetings should be made into a series and archived so that they can be accessed for learning anytime.
- Strengthen promotion and dissemination through social media and YouTube and devise ways to improve outreach to a diverse range of professionals.
- Introduce a workshop-style session in which participants can discuss with one another, aimed at SMEs and those hearing about GCBPR for the first time.
- After the event, operational support should be strengthened, such as by updating the FAQs to reflect the opinions expressed by the participants and during the Q&A session, instead of simply providing a report of the event.
- Provide thorough follow-up materials and information regarding the consultation desk after the seminars and ensure a seamless flow from participation to consultation (in conjunction with website improvement measures).

(3) Brochures and leaflets

- At the time of preparing this report, relevant advertising material was not available. Therefore, on a trial basis, create highly visible brochures or leaflets that will be useful for internal presentations, such as a sheet using images and illustrations that encourages people to take one, or a trifold version that includes the system outline, and devise distribution locations and media to ensure they reach a wider audience.
- Ensure that the materials provide more than a system overview, including content obtained from the survey interviews, such as case examples of SMEs and specific business sectors, the man-days required for the certification, the organizational system necessary for maintaining certification, and information that visualizes cost-effectiveness.
- Request material to be placed at government and public agencies, local governments that provide support to business operators with overseas subsidiaries, and those that are considering expansion.

Overall, the design of websites for the competent authorities and the assessment body and the links they contain should be devised so that information is seamlessly linked, from the system overview to its practical implementation, along with support for the application process.

Table 32 shows the specific initiatives identified through the improvement measures and KPIs used to evaluate their effectiveness.

Table 32 Effective Specific initiatives and evaluation indicators for public relations and outreach activities

Target	Initiative	KPI
[1] Websites	**1. Enhance the dissemination of information in English** - Introduce the activities of the Global CBPR Forum and the role of the Accountability Agent (AA) in Japan (JIPDEC) **2. Provide case examples for overseas users** - Emphasizing the benefits of smooth data collaboration with Japanese companies **3. Provide explanatory materials and information about the system in multiple languages** - Clarify the system's objective, certification, and international positioning (develop websites)	• Number of overseas inquiries • Number of certification applications by overseas companies (Japanese subsidiaries) • Page views of English-language sites • Number of leads acquired at international conferences
	4. Deliver easy-to-understand videos and visual content. - Explain GCBPR and why certified organizations can be considered reliable	• Awareness survey of certification marks and systems • Number of views
	5. Run social media campaigns - To raise awareness of the importance of protecting personal data. - Improved recognition of certification marks	• Social media engagement (likes, shares, and comments)

Target	Initiative	KPI
	6. Gain media exposure (news and magazines) - Deliver news of system launches and increases in the number of certified organizations	• Amount of media coverage
	7. Release of technical documentation and assessment guidelines - Enhancing transparency and promoting entry	• Page views • Number of downloaded guidelines
	8. Deliver seminars and symposia - Offers unlimited archive delivery - Make the distributed material available for download	• Number of views • Number of material downloads
[2] Seminars and symposia	**1. Hold seminars and webinars by industry.** - Target industries such as IT, e-commerce, finance, and SaaS, where many cross-border data transfers occur. - Present the latest information from the competent authorities (i.e., the Personal Information Protection Commission and METI) and the assessment body (JIPDEC)	• Number of seminar participants and satisfaction level • Increase in the number of certification applications • Industry coverage expansion by certified companies • Trend in the number of inquiries
	2. Provide examples of the benefits of certification - Introduce companies that are already certified (e.g., Japanese certified organizations and companies certified by AAs in other jurisdictions) - Emphasizing enhanced trustworthiness when expanding overseas operations and meeting business partners' requests	
	3. Conduct workshops for SMEs - Discuss practical issues, introduce actual cases of SMEs becoming certified and gaining benefits, build an image of becoming certified, and provide an overview.	• Number of seminar participants • Distribution of participant attributes and rate of change
[3] Brochures and leaflets	**1. Prepare brochures and leaflets** - System overview, application procedures and flow, and case examples. Present them in a format that is easy to understand for first-time readers.	• Number of copies issued and distribution points
	2. Provide a checklist and guidebook - Visualization of the certification process, establishment of the necessary system, and cost-effectiveness	• Number of guidebook downloads

3. Points to Note During Public Relations and Outreach Activities

3.1. Setting the Priority Targets

(1) Management system certified organizations

Targeting those with the PrivacyMark and ISMS that were covered in the 2024 Research as well as PIMS that is part of this research would be effective. Business operators that have already obtained one of the management system certifications have a foundation in place needed to comply with the GCBPR program requirements. They have experience with third-party certification, and knowing that GCBPR is necessary to meet their needs will be the driving force for them to become certified.

These certified organizations are expected to be positioned as priority targets. By clearly communicating that obtaining GCBPR is not a major hurdle if the existing management system infrastructure is utilized and alignment rate figures are used as the basis, business operators can be expected to transition to the consideration stage. In addition, effective promotion toward the system adoption will be possible by providing information tailored to the business operator's individual circumstances (existing certifications, business activities, actual status of cross-border transfers, etc.).

(2) Targeting based on business operator attributes

The questionnaire results suggested that the target should be the following business operators to increase efficiency in promoting the system adoption

- Business operators that actively use cloud services
- SaaS providers and other cloud service providers
- Those in the manufacturing industry planning to expand into the Asian region
- Wholesalers and retailers engaged in cross-border e-commerce
- Tier 0[34] business operators that influence a particular business field, such as manufacturing.

Many business operators, regardless of size or industry, use cloud services. However, since it is common for business operators to use services based only on the provider's terms and conditions without entering into a contract, requesting or confirming that the information handling be the same as their own is difficult. Several interviewees also reported cases in which detailed information was not disclosed.

Thus, cloud service providers can be positioned as strong candidates for obtaining GCBPR since having them become certified can be used to persuade service providers and service users alike that the system is beneficial for them.

3.2. Raising Awareness and Promoting Basic Understanding

(1) Raising awareness of unconscious cross-border transfers

The results of the interviews revealed that many business operators believe that their companies do not conduct cross-border transfers; however, cross-border transfers do in fact occur through the use of cloud services (e.g., AWS, Google Cloud, Box, and OneDrive). Business operators pointed out that awareness of information being transferred overseas through the use of cloud services is very low and that business operators conducting operations only in Japan do not accept it.

Raising awareness of such unconscious cross-border transfers is a prerequisite for business operators to understand the need for GCBPR. Communicating to cloud service users in an easy-to-understand manner the possibility that they may be undergoing cross-border transfers and what kind of response is required in such cases is considered an effective entry point for encouraging consideration into obtaining GCBPR.

[34] Manufacturers in the automobile industry. Other examples include the finance and healthcare industries.

(2) Providing information to move business operators from awareness to consideration

The type of information that business operators interviewed cited as necessary to shift their mindset from recognition to consideration was as follows: specifically, what types of business requires certification; the size of business operators that have become certified; and what benefits those operators feel they have received.

In addition to a general explanation of the system, it can be effective to provide information that enables business operators to determine why their company needs to be certified (judgment criteria, self-check tools, etc.) to facilitate their transition to the consideration stage. As multiple certification systems exist, sorting out and providing information on the relationship between the GCBPR and other systems (e.g., PrivacyMark, ISMS, and METI's security rating system), as well as the benefits and drawbacks, are also considered to be key support factors in helping business operators determine priorities in obtaining various certification systems.

(3) Raising awareness of SME eligibility for certification

The interviewees commented that only large corporations appear to be certified currently, which does not serve as a useful reference for them and feels irrelevant to their company. The fact that currently certified organizations in Japan are mostly major corporations is a potential psychological barrier for SMEs, making it difficult for them to consider the relevance to their own businesses.

Some respondents also suggested that it would be easier to understand that SMEs are able to obtain certification if it were shown not only through text-based information but also using actual case examples of businesses and their testimonials, along with diagrams and illustrations. The AA questionnaire also confirmed that some AAs offer discounts to small business operators as a measure to target SMEs.

When cases arise going forward of SMEs obtaining certification, actively disseminating them should be effective in broadening perception by business operators that they can also obtain certification. It is also effective to actively disseminate discounts to small business operators if they become available.

(4) Websites

The interviewees also expressed their views that it would be extremely helpful if they could receive information on foreign laws and regulations, as they differ from country to country, and it is difficult to keep up with legal amendments. They would also like to receive information, such as reports on seminars and reporting by the participants.

Personnel in charge of handling personal information use the websites of ministries and agencies to collect information. Therefore, the number of visitors to GCBPR pages is expected to grow by placing banners guiding users to dedicated GCBPR pages and adding links to these pages in the submenus of the websites of the competent authorities. The effectiveness of seminars and networking events can be measured by creating a landing page[35] and announcing each event individually.

3.3. Outreach Methods

[35] Refers to a web page where a visitor first arrives from an advertisement or search result. It is usually a vertical single-page, purpose-specific design specialized in prompting a user's specific action (conversion), such as requesting information or making a purchase.

With the current situation where the level of awareness is extremely low, it is considered effective to utilize two types of media: online and paper-based. These include search-linked advertising and leaflet distribution, which can efficiently reach business operators that potentially have an interest in GCBPR.

Search-linked advertising accounts for about 40% of internet advertising expenditure. It is advantageous because its effectiveness is easy to measure and its budget is easy to manage. Paper media reaches those less familiar with digital technology and is highly visible. By limiting distribution points to specific target groups, it is also easy to operate within a set budget.

To fully leverage these measures, a dedicated GCBPR website must be created. Continuous maintenance will be required because it is important for visitors who come from search-linked advertisements or paper media to obtain useful information and have access to the latest updates.

IV. Other

1. Recommendations Regarding System Design

1.1. Improving the Review Efficiency

In interviews with certified organizations, their responses regarding system improvements indicated that the number of man-days required to prepare documents decreases as familiarity and know-how accumulate, with the work in the first year being the heaviest. Some participants also commented that they did not know what supporting documentation was required for the 50 questions.

The eight companies, excluding certified organizations, are business operators that have obtained the PrivacyMark or ISMS, and free review fees may be insufficient as an incentive for certification. Seven companies raised concerns about the number of man-days, labor, and maintenance required after becoming certified. As the labor, cost, and maintenance of the certification system are issues for almost all business operators, it is vital to streamline the GCBPR assessment process and consider ways to improve assessment efficiency in comparison with the specifically applicable PrivacyMark, ISMS, and PIMS systems. Mechanisms for sharing practical know-how of certified organizations, such as differences in man-days between the initial certification and recertification, as well as points to be addressed according to the type of business, could also be useful in supporting the decision-making process of business operators considering certification.

To increase incentives for more business operators to obtain GCBPR, simplifying the existing assessment process and reducing the number of man-days to accommodate cases in which multiple certifications have already been obtained can lower the barrier to certification, which will have a significant impact in increasing the number of certified organizations.

1.2. Expansion of the Certification Unit and Scope of Review

GCBPR is a corporation-based certification that makes it easier for organizations to earn trust. As of the time this research was conducted, AAs in the Republic of Korea, Chinese Taipei, and Japan provide certification only on an individual company basis. However, for AAs in the U.S. and Singapore, the audit scope can be selected on an individual company basis or to include group companies.

The Global PRP operations also have differences among AAs, as is the case with certification units, where only those in the U.S. and Singapore conduct assessments among all of the AAs. The interview results suggested that business operators feel that the Global PRP, with its clearly defined scope of assessment for processors, may be a good option.

It is clear from the interviews that this system flexibility provides an incentive for applicant organizations to obtain certification. Under the current system, differences exist in the assessment provided even within the same certification system. Government bodies and AAs that serve as points of contact for the certification system are expected to actively work to promote efforts that respond to the needs of business operators, including clarifying how the program requirements relate to the enforcement of domestic law being enforced.

1.3. Creation of External Factors (Medium-to-Long-Term Initiatives)

The results of the interviews strongly suggest that the decision of business operators to obtain certification is greatly influenced by external factors. Business operators commented that if they

were told that certification was required for doing business, they would definitely obtain it. They also suggested that large companies asking their business partners to obtain GCBPR would spread certification quickly and that if it were a bidding requirement, they would be forced to get certified.

Measures to create external factors to serve as a major driver for expanding certification in Japan, such as encouraging business operators with global operations and considering incorporating certification as bidding requirements for public procurement, are also indispensable factors as initiatives apart from public relations and outreach.