(Appendix)

Check Sheet for Cybersecurity Self-Assessment (FY2022)

Involvement of executives concerning cybersecurity

[Q1] Choose the applicable one regarding your organization's management policy and management plans concerning cybersecurity.

	Answer column
1. Have set up a management policy to ensure cybersecurity and have formulated plans for achieving it with the involvement of chief executive (president, CEO, etc.)	
2. Have set up a management policy to ensure cybersecurity with the involvement of chief executive (president, CEO, etc.), but have yet to formulate plans for achieving it	
3. Planning to set up a management policy to ensure cybersecurity	
4. Have no plan to set up a management policy to ensure cybersecurity	

[Q2] Choose the applicable one regarding personnel in charge of cybersecurity at your organization.

	Answer column
1. An executive solely in charge of cybersecurity (CISO, etc.)	
2. An executive who administers system risks (including cybersecurity)	
3. An executive who administers matters other than system risks (including cybersecurity)	
4. Multiple executives (in charge of the cybersecurity affairs within the scope under their administration)	
5. Staff of a department in charge of managing system risks (including cybersecurity) (other than an executive)	
6. Staff of a department other than a department in charge of managing system risks (including cybersecurity) (other than an executive)	
7. There are no personnel in charge of cybersecurity.	

[Q3] Choose all applicable regarding the contents concerning cybersecurity that are periodically reported to executives.

Contents periodically reported	Answer column (1: Yes; 2: No)
1. Occurrences of cyber incidents within the organization	
2. Occurrences of cyber incidents at group companies	
3. Occurrences of cyber incidents at other companies (including trends relating to cyberattacks)	
4. Results of the monitoring concerning targeted emails and unauthorized communications, etc.	
5. Information concerning vulnerability	
6. Assessment concerning cybersecurity (including assessment by a third party)	
7. Progress of cybersecurity controls	
8. Status of conducting training with the assumption of a cyber incident	
9. Status of conducting education and awareness-raising activities targeting executives and staffs	
10. Other (Write details in the free column.)	
11. Periodic reports concerning cybersecurity are not made to executives.	

If you chose "1: Yes" for "10. Other," please write details in the free column below.

[Q4] Choose all applicable regarding the contents concerning cybersecurity that are reported on an ad-hoc basis to executives.

Contents reported on an ad-hoc basis	Answer column (1: Yes; 2: No)
1. Serious incidents that occurred in the organization's systems	
2. Serious incidents that occurred at other companies and may affect the organization	
3. Serious vulnerability (including inappropriate design or settings) found in the organization's systems	
4. Other (Write details in the free column.)	
5. Reports are not made on an ad-hoc basis to executives.	

If you chose "1: Yes" for "4. Other," please write details in the free column below.

Identifying and responding to risk concerning cybersecurity

[Q5] Choose all applicable regarding accidents, etc. due to cyberattacks to your organization.

Note: This question is common to the FISC questionnaire survey. Please see "Common questions with FY2022 The Center for Financial Industry Information Systems (FISC) questionnaire survey" on page 1.

Details of the accidents, etc.	Answer column (1: Occurred; 2: Not occurred)
1. Information leakage due to infection by a computer virus, etc.	
2. Information leakage due to the abuse of a vulnerability	
3. Service suspension due to a DoS/DDoS attack	
4. Unauthorized falsification of the organization's website	
5. Encryption or destruction of a system or data by ransomware	
6. Damage due to an illegal remittance in an internet transaction, etc.	
7. Damage other than the above due to infection by a computer virus, etc.	
8. Other	
9. There has been no accident, etc.	

If you chose "1: Occurred" for "8. Other," please write details in the free column below.

[Q6] Choose all applicable regarding collection of cybersecurity-related information.
Note: This question is common to the FISC questionnaire survey. Please see "Common questions with FY2022 FISC questionnaire survey" on page 1.

Information source	Answer column (1: Yes; 2: No)
1. From the FISC's "Cybersecurity Incident Information"	
2. From prefectural polices	
3. From bodies that collaborate diversely for responding to cyberattacks(*1)	
4. From companies to which the organization outsources cyberattack monitoring, and system integrators, security vendors, etc.	
5. By using threat intelligence services,(*2) etc.	
6. By attending various seminars	
7. From the internet, newspaper, etc.	
8. From group companies	
9. From industry associations	
10. From other sources	
11. Do not conduct information collection activities	

*1 Bodies that collaborate diversely for responding to cyberattacks refer to the National center of Incident readiness and Strategy for Cybersecurity (NISC), Financials ISAC Japan, JPCERT Coordination Center, Japan Cybercrime Control Center (JC3), etc.

*2 Threat intelligence services are services to analyze information that exists in cyberspace, including dark websites, and provide individual financial institutions separately with information that they should be aware of at an early stage.

If you chose "1: Yes" for "10. From other sources," please write details in the free column below.

[Q7] Choose all applicable regarding the status of conducting a risk assessment concerning cybersecurity with regard to material systems* that your organization is using.
* Material systems are systems that an organization recognizes as especially important in its business operations, such as accounting systems and systems handling customer information.

Measures	Answer column (1: Yes; 2: No)
1. Conduct a risk assessment when introducing a new system or conducting a large-scale renewal	
2. Regularly conduct a risk assessment	
3. Timely conduct a risk assessment (each time an increase in cybersecurity risks is recognized)	
4. Irregularly conduct a risk assessment (there is no policy on when to conduct an assessment)	

[Q8] Choose the applicable one regarding decisions on responses to cybersecurity risks and prioritization of these responses.

1. The need for making responses to risks (reduction, avoidance, transfer, or acceptance) and prioritization of these responses are decided on each occasion of conducting a risk assessment as judged by executives.	Answer column

2. The need for making responses to risks (reduction, avoidance, transfer, or acceptance) and prioritization of these responses are decided on each occasion of conducting a risk assessment as judged by the department in charge of managing system risks (including cybersecurity).	
3. The need for making responses to risks (reduction, avoidance, transfer, or acceptance) and prioritization of these responses are decided on each occasion of conducting a risk assessment as judged by the department in charge of	
4. Responses (reduction, avoidance, transfer, or acceptance) based on the results of risk assessments are not made.	

Audit concerning cybersecurity

[Q9] Choose all applicable regarding the subjects of an audit concerning cybersecurity.

Audit subject	Status of conducting an audit (1: Conducting; 2: Planning; 3: Have no plan)	
	1. Verification by internal personnel (internal audit department)	2. Verification by an external body*
1. Appropriateness of executives' involvement		
2. Appropriateness of compliance with related laws and regulations and rules		
3. Appropriateness of risk assessments		
4. Status of compliance with rules and procedures concerning security measures		

* An external body means an audit firm or a consulting firm, etc.

[Q10] Choose all applicable regarding destinations to which the results of an audit concerning cybersecurity must be reported, other than audited departments.

Where to report audit results	Answer column (1: Yes; 2: No)
1. Board of directors, governing board	
2. Audit committee	
3. Management council	
4. President, CEO, etc.	
5. Other (Write details in the free column.)	
6. The results are reported only to audited departments.	

If you chose "1: Yes" for "5. Other," please write details in the free column below.

[Q11] Choose the applicable one regarding how the audit department confirms the status of improvements made by audited departments for matters pointed out concerning cybersecurity.

Measures	Answer column (1: Yes; 2: No)
1. The audit department receives reports on the improvement results.	
2. With regard to recommendations for remedial measures that are highly important, the audit department conducts an examination to confirm the improvement results.	

Education and training concerning cybersecurity

[Q12] Choose all applicable regarding the status of calling attention to and providing education and training concerning cybersecurity.

Targeted personnel	Occasionally call attention (1: Yes; 2: No)	Regularly provide e-learning (including learning using videos and documents, etc.) for awareness-raising (1: Yes; 2: No)	Conduct training against targeted emails (1: Yes; 2: No)	Conduct training with the assumption of infection by malware, etc.* (1: Yes; 2: No)
1. Executives				
2. Staff members of a specialized body for making responses to cyber incidents (CSIRT, etc.)				
3. Staff members of the department in charge of systems				
4. Staff members of the operation department (system users, etc.)				
5. Staff members of other departments (public relations department, etc.)				

Targeted personnel	Occasionally call attention (1: Yes; 2: No)	Confirm the status of conducting training, etc. (1: Yes; 2: No)
6. Outsourcees		
7. Customers		

*Training for initial responses in the event of infection by malware, etc.

Evaluation of new digital technologies

[Q13] Choose the applicable one regarding the status of securing human resources who can assess cybersecurity risks that may arise as a result of introducing new digital technologies.

1. Have secured personnel sufficiently by utilizing only internal staff members (including reshuffling of personnel from other departments)
2. Have secured personnel sufficiently by utilizing outside human resources (including those from the parent company, etc.), in addition to internal staff members
3. Have secured personnel sufficiently by utilizing only outside human resources
4. Have not secured personnel sufficiently

Answer column

[Q14] Choose all applicable regarding the introduction of new digital technologies and the matters you recognize as a cybersecurity threat associated with the introduction. Even if you have not introduced any new digital technologies, choose the matters you recognize as a possible cybersecurity threat associated with the introduction.

	Whether having introduced or not (1: Have introduced; 2: Have not introduced)	Matters you recognize as a cybersecurity threat associated with the introduction (1. Recognize as a threat*; 2: Do not recognize as a threat)			
		Destruction or falsification	Outage	Information leakage	Other
1. Public cloud services					
2. Open APIs (Write)					
3. Open APIs (Read)					
4. Smartphones and tablets					
5. Systems for teleworking					

*Irrespective of whether you are taking any countermeasures, if you recognize that there is a threat, choose "1: Recognize as a threat."

If you chose "1: Recognize as a threat" for the option "Other," please write details in the free column below.

Asset management

[Q15] Choose the applicable one respectively regarding the status of maintaining a management register, etc. for internal systems and external systems.*
* Internal systems are systems operated within the own organization.
External systems are systems operated outside the own organization (including cloud services).

1. Have prepared a register, etc. and update them each time there is any change, and regularly check the content of the register
2. Have prepared a register, etc. and update them each time there is any change
3. Have prepared a register, etc. and regularly check the content of the register
4. Have prepared a register, etc. and irregularly check the content of the register
5. Have prepared a register, etc. but have not updated it
6. Have not prepared a register, etc.

(i) Internal systems: Answer column

(ii) External systems: Answer column

[Q16] Choose the applicable one respectively regarding the status of maintaining a management register, etc. in which product names and versions, etc. are entered for the purpose of appropriately managing (i) hardware and (ii) software in your organization.

1. Have prepared a register, etc. and update it each time there is any change, and regularly check the content of the register
2. Have prepared a register, etc. and update it each time there is any change
3. Have prepared a register, etc. and regularly check the content of the register
4. Have prepared a register, etc. and irregularly check the content of the register
5. Have prepared a register, etc. but have not updated it
6. Have not prepared a register, etc.

(i) Hardware: Answer column

(ii) Software: Answer column

[Q17] Choose the applicable one regarding the status of maintaining a network connection diagram* of your organization.

* A diagram which shows the structure of the network and connections between systems within the organization

	Answer column
1. Have prepared a connection diagram and update it each time there is any change, and regularly check the content of the connection diagram	
2. Have prepared a connection diagram and update it each time there is any change	
3. Have prepared a connection diagram and regularly check the content of the connection diagram	
4. Have prepared a connection diagram and irregularly check the content of the connection diagram	
5. Have prepared a connection diagram but have not updated it	
6. Have not prepared a connection diagram	

Access control

[Q18] Choose all applicable regarding the granting of accounts and access rights to material systems.

Measures	Answer column (1: Yes; 2: No)
1. Grant accounts to the minimum necessary personnel	
2. Grant an access right to each user within the minimum necessary range for business (permit only reference or permit data update, etc.)	
3. Grant an access right only for a limited term of validity	
4. Renew access rights each time someone retires, a personnel change is made, or the organizational structure is altered	
5. Regularly check the settings of access rights	

[Q19] Choose all applicable regarding the control of remote access to material systems.

Measures	Answer column (1: Yes; 2: No)
1. As operational management when making remote access (logging in) to material systems from outside, checking and restricting the connection source and monitor the connection, etc.	
2. Have introduced a mechanism of multi-factor authentication for making remote access (logging in) to material systems from outside	
3. Have obtained access logs for the purpose of preventing unauthorized access or information leakage	
4. Have put in place measures in preparation for a case where a staff member has lost their authentication device (access token, IC card, etc.) that is necessary for identity verification upon making an access.	
5. Restricting material systems that allow remote access	
6. Are not allowing remote access	

Data protection

[Q20] Choose all applicable regarding measures for data protection.

Measures	Answer column (1: Yes; 2: No)
1. Encrypt material data*	
2. Control access to material data	
3. Control downloading and printing of material data (including a measure to record operation logs when downloading and printing data)	
4. Control copying of data into external storage device	
5. Have introduced a mechanism to automatically encrypt data when transmitting them to external organizations, etc.	

* Material data are those including information for which strict management is required, such as information that may cause a serious impact on business if it is leaked, information that will cause a serious impact on the execution of operation if it is damaged or otherwise becomes unavailable, and information that is required to be managed in compliance with laws and regulations.

[Q21] Choose all applicable regarding measures with the assumption that backup data in a material system are destroyed or falsified by ransomware, etc.

Measures	Answer column (1: Yes; 2: No)
1. Store multiple generations of backup data	
2. Store backup data offline or by any other method that does not allow direct access from the network	
3. Store backup data in a non-rewritable and non-deletable medium	
4. Other (Write details in the free column.)	
5. None is applicable.	

If you chose "1: Yes" for "4. Other," please write details in the free column below.

Log management

[Q22] Choose all applicable regarding rules concerning audit trails (logs) for material systems.

Rules	Answer column (1: Yes; 2: No)
1. There are rules concerning logs to be obtained.	
2. There are rules concerning the log retention period.	
3. There are rules to prohibit alteration and deletion of logs without permission.	
4. There are provisions to require regular checking of logs to confirm that there is no wrong act.	
5. There are no rules concerning audit trails (logs) for systems.	

Vulnerability management

[Q23] Choose the applicable one respectively regarding the timing of conducting a vulnerability assessment or otherwise inspecting the effectiveness of measures against attacks from outside or inside to the systems that your organization is using (when outsourcing system operations, including a case where you check the outsourcees' implementation of an assessment, etc.).
When you do not provide a website (website open to customers) or internet banking services, choose "6. Do not provide services."

1. Conduct an assessment regularly, and also when introducing a new system or conducting a large-scale renewal
2. Regularly conduct an assessment
3. Conduct an assessment when introducing a new system or conducting a large-scale renewal
4. Irregularly conduct an assessment (there is no policy on when to conduct an assessment)
5. Do not conduct an assessment
6. Do not provide services

	By type	
Subject	Vulnerability assessment (Web application)	Vulnerability assessment (platform)
Office automation environment*		
Website (website open to customers)		
Internet banking system		

* Please respond regarding vulnerability assessments targeting the following.
- Website browsing systems (a system that provides a virtual browser or internet virtual terminal, and Proxy, DNS, etc. that are necessary for internet connection)
- Email systems and file servers
- Devices essential for the security of the internal environment (active directory servers, etc.)

[Q24] Choose the applicable one respectively regarding the status of conducting a penetration testing(*1) and a threat-led penetration testing.(*2)

*1 A penetration testing is a test for checking whether penetration or falsification is possible and whether any attack can be detected and for verifying the promptness and appropriateness of responses by launching simulated attacks by means such as using simulated malware or abusing a vulnerability or a defect in settings.

*2 A threat-led penetration testing is a more practical test for checking whether penetration or falsification is possible and whether any attack can be detected and for verifying the promptness and appropriateness of responses by launching simulated attacks imitating strategies and means that attackers are supposed to adopt, after first analyzing risks faced by the organization individually and specifically.

1. Have conducted a test twice or more
2. Have conducted a test once and plan to conduct the next test
3. Have conducted a test once but have no plan to conduct the next test
4. Considering conducting a test (have yet to conduct a test)
5. Have no plan to conduct a test

Test type	Answer column
Penetration testing	
Threat-led penetration testing, etc.	

[Q25] Choose the applicable one respectively regarding policies for applying a patch when serious vulnerability is found in your organization's systems.

1. Apply a patch as promptly as possible

Systems and terminals	Answer column

2. Apply a patch at a timing of maintenance, etc.	
3. Apply a patch at the time of renewal of systems	
4. Do not apply a patch in principle	

Systems and terminals connected to the internet*	
Systems and terminals unconnected to the internet	

* Including a case where there are communications with a system that is connected to the internet.

[Q26] Choose the applicable one regarding responses when you do not apply a patch against a serious vulnerability (only take a measure to avoid influence of the vulnerability <workaround, such as disablement of a specific function>, or make no responses to the vulnerability).
If you apply patches fully to all serious vulnerabilities, please answer by assuming a case where you do not apply a patch.

	Answer column
1. The executives who administers system risks (including cybersecurity) approves the determination that the risk of not applying a patch can be tolerable. 2. The department in charge of managing system risks (including cybersecurity) approves the determination that the risk of not applying a patch can be tolerable. 3. The department in charge of the relevant system approves the determination that the risk of not applying a patch can be tolerable. 4. The risk of not applying a patch is not taken into consideration.	

Technical measures against cyberattacks

[Q27] Choose all applicable regarding measures against cyberattacks taken for OA terminals.*
* OA terminals are standard terminals that staff members normally use for preparing documents, etc.

Measures	Answer column (1: Yes; 2: No; 3. Don't know)
1. Separate the network of OA terminals and the internet (including the use of a virtual browser or other logical means)	
2. Restrict websites that can be accessed from OA terminals	
3. Restrict the rights to execute software of OA terminals to the minimum necessary (for example, the department in charge of systems manages the administrator rights)	
4. Have introduced a signature-based anti-malware product to OA terminals	
5. Have introduced a behavior-based anti-malware product (including EDR) to OA terminals	
6. Restrict connections of external storage device to OA terminals	
7. Have restricted access points to connect OA terminals in advance (restrict unauthorized wireless communications, etc.)	
8. Have introduced a mechanism of multi-factor authentication	

[Q28] Choose all applicable regarding measures against cyberattacks taken at the border between your organization and the outside.

Measures	Answer column (1: Yes; 2: No; 3. Don't know)
1. Control access by using a firewall	
2. Detect and prevent unauthorized communications by using IDS/IPS*	
3. Filter emails containing suspicious files or links	
4. Inspect the content of the encrypted SSL/TLS communications from the outside by decrypting them	
5. Block communications that do not go through a proxy server	
6. Control access by using an authentication function	

* Intrusion Detection System (IDS) is a system that monitors communications on the network and detects and reports unauthorized intrusion and suspicious malware communications, etc.
Intrusion Prevention System (IPS) is a system with a function to automatically block detected unauthorized communications.

[Q29] When you provide a website (website open to customers) or internet banking services, choose all applicable respectively regarding measures against cyberattacks taken for each of them.
When you do not provide a website (website open to customers) or internet banking services, choose "4. Do not provide services."

Measures Answer column (1: Yes; 2: No; 3: Don't know; 4. Do not provide services)	Website (website open to customers)	Internet banking system
1. Control access by using a firewall		
2. Detect and prevent unauthorized communications by using IDS/IPS*		
3. Detect and block unauthorized communications by using WAF*		
4. Detect falsification of the website		

5. Monitor system resources (network traffic volume, memory, etc.)		
6. Have introduced measures against DoS/DDoS attacks (load balancing services such as content delivery network by communications companies, etc.)		

* Web Application Firewall is software or hardware that analyzes the content of http communications (including https communications) between a website and users and automatically blocks attacks or other unauthorized communications.

Detection

[Q30] Choose the applicable one regarding a body that conducts monitoring and analysis of cybersecurity-related issues (such as SOC (including a case of outsourcing the monitoring and analysis)).

	Answer column
1. Have established a body (monitoring and analysis are being conducted 24 hours a day, 365 days a year) 2. Have established a body (monitoring and analysis are not conducted 24 hours a day, 365 days a year) 3. Have a plan to establish a body or considering establishing a body 4. Have no plan to establish a body	

[Q31] Choose all applicable regarding targets monitored by an SOC or other department that monitors cybersecurity-related issues.

Targets for cybersecurity monitoring	Answer column (1: Yes; 2: No)
1. Status of the detection of or the infection with malware	
2. Status of receiving emails with files	
3. Status of browsing external websites	
4. Status of communications from the outside (including communications to the website open to customers)	
5. Status of communications to the outside	
6. Status of internal communications	
7. Status of connections of external storage device such as USB flash drive	
8. Status of connections to the organization's systems by outsourcees that handle material information or business operations	
9. Status of connections of terminals to the organization's internal network	
10. Status of nonconformity when conducting analyses by correlating various logs (suspicious activities)	

Incident response and recovery

[Q32] Choose the applicable one regarding staff for making responses (including your parent company, etc.) upon a cyber incident.

	Answer column
1. Have established a permanent specialized body for making responses to cyber incidents (CSIRT, etc.) 2. Have not established a permanent specialized body, but have appointed staff members in advance to have them make responses upon a cyber incident 3. Have not decided staff members who will make responses upon a cyber incident	

[Q33] Choose all applicable regarding the policy of offering cooperation (information provision) to external organizations (Financials ISAC Japan, etc.).

Policy of cooperation	Answer column (1: Yes; 2: No)
1. Provide information on cyber incidents that occurred within the organization	
2. Provide information on suspicious communication destinations that the organization observed	
3. Provide the characteristics of attacks that the organization ascertained	
4. Provide information on cyberattack warnings, etc. that the organization recognized	
5. Provide information on targeted emails that the organization received	
6. Do not provide information	

[Q34] Choose all applicable regarding the formulation of rules and procedures for preventing the spread of damage upon a cyber incident.

Status of formulation	Answer column (1: Yes; 2: No)
1. Have formulated rules and procedures to separate systems from the relevant network promptly at the stage when infection by malware is suspected	
2. Have formulated rules and procedures to block the source of access and separate systems from networks that can be access routes promptly at the stage when unauthorized access is suspected	
3. Have formulated rules and procedures to freeze the relevant account and separate systems from networks that can be access routes promptly at the stage when an unauthorized login is suspected	

4. Have formulated rules and procedures to shut down systems based on the background of a cyber incident	
5. Have not formulated rules and procedures for preventing the spread of damage	

[Q35] Choose the applicable one regarding the status of strengthening frameworks based on past responses to incidents (including training and exercises).

	Answer column
1. In light of past responses to cyber incidents, update frameworks (rules, structures for information liaison, contingency plans, and the number of personnel, etc.) and technical measures as necessary 2. In light of past responses to cyber incidents, update only structures as necessary 3. In light of past responses to cyber incidents, update only technical measures as necessary 4. Do not update structures and technical measures in light of past responses to cyber incidents 5. Have no record of making responses to cyber incidents	

[Q36] Choose the applicable one respectively regarding the content of contingency plans by type of cyberattacks (damage) from the perspective of enhancing cyber resilience (ability to respond to and recover from damage in the event of a cyber incident).

[Whether having formulated contingency plans against attacks]

1. Have formulated contingency plans by type of cyberattacks (damage) (1: Yes; 2. No)
   * If you chose "2: No," you do not need to answer to 2. to 5. below.
2. Have set the recovery time objective (1: Yes; 2. No)
3. Contingency plans include measures with the assumption that outsourcees become subject to cyberattacks (1: Yes; 2. No)

[Status of conducting training and exercises of contingency plans]

4. Have conducted training and exercises by type of cyberattacks (1: Yes; 2. No)
5. Outsoucees also participate in training and exercises regarding contingency plans (1: Yes; 2. No)

Cyberattacks (damage)	Content of contingency plans				
	1	2	3	4	5
1. Destruction or falsification of systems					
2. System outage					
3. Information leakage					

[Q37] Choose all applicable regarding whether you have formulated procedures (manual, etc.) for reporting to the relevant parties upon the occurrence of a cyberattack (damage). For only "4. The organization's group companies," you may choose "3: No applicable target."

Target to report	Answer column (1: Yes; 2. No; 3: No applicable target)
1. Ministries and agencies concerned, The Bank of Japan	
2. Customers	
3. Outsourcees	
4. The organization's group companies	
5. Outside people in general (including mass media)	

Management of third parties

[Q38] Choose the applicable one regarding the status of conducting a risk assessment concerning cybersecurity of third parties.(*1)
Choose answers regarding outsourcees and third parties excluding outsourcees(*2) respectively in the relevant answer columns.

*1 A third party is another organization with which the organization has a business relationship or has concluded an agreement, etc. for providing services (ex. an information system subsidiary, an outsourcee such as a system vendor, a service provider such as a cloud service provider, a fund transfer service provider, etc.).
*2 Third parties excluding outsourcees are third parties with which the organization has not concluded an outsourcing agreement.

Status of conducting risk assessment	Answer column for outsourcees (1: Yes; 2. No)	Answer column for third parties excluding outsourcees (1: Yes; 2. No)
1. Conduct a risk assessment concerning cybersecurity when selecting a third party		
2. Regularly conduct a risk assessment concerning cybersecurity even after selecting a third party		

[Q39] Choose the applicable one regarding the status of managing cybersecurity risks for important third parties.*

* An important third party is a third party which the organization recognizes as being important for its business operations.

	Answer column
1. The supervisory department centrally conducts management concerning cybersecurity risks for important third parties and services provided by them. 2. Each department conducts management concerning cybersecurity risks for important third parties and services provided by them. 3. Cybersecurity risks for important third parties and services provided by them are not managed.	

[Q40] Choose all matters that are prescribed from the perspective of cybersecurity in agreements, etc. with third parties.
Choose answers regarding agreements, etc. with outsourcees and agreements, etc. with third parties excluding outsourcees respectively in the relevant answer columns.

Matters prescribed	Answer column for outsourcees (1: Yes; 2. No)	Answer column for third parties excluding outsourcees (1: Yes; 2. No)
1. Boundaries of responsibilities for cybersecurity controls in outsourced operations or services to be provided		
2. Personnel responsible for the management of cybersecurity risks		
3. Cybersecurity controls to be taken		
4. Responses in the event of an incident		
5. Permission of the organization's on-site investigations		
6. Reporting to the organization when a third party recontracts with another third party for the outsourced operations that may affect the organization's cybersecurity		

[Q41] Choose all applicable respectively regarding the status of management and monitoring of cybersecurity for your organization, overseas bases, affiliated companies and outsourcees.

Organization	(i) Whether there is any applicable organization (1: Yes; 2: No) If you chose "2: No," you do not need to answer to (ii) Status of compliance with the organization's security policy and (iii) Status of monitoring regarding (ii).	(ii) Status of compliance with the organization's security policy (Choose one) 1. Confirm that the organization's security policy is satisfied (observed)* 2. Recognize that the organization's security policy is not satisfied (some policies are not followed) 3. Do not catch the status of managing cybersecurity	(iii) Status of monitoring regarding (ii)	
			Evaluate the status of cybersecurity controls (including inspections and audit, etc.) to be carried out by applicable organizations (1: Yes; 2: No)	Use services that conduct evaluation, analyses and rating, etc. concerning applicable organizations' cybersecurity (1: Yes; 2: No)
1. Domestic bases (headquarters, head office and branches, business offices, etc. in Japan)				
2. The organization's overseas bases				
3. IT-related subsidiaries and group companies				
4. Subsidiaries and group companies excluding IT-related ones				
5. Outsourcees (excluding cloud service providers)				
6. Companies to which open APIs are connected				
7. Cloud service providers				
8.Businesses with which the organization collaborates on payment services, such as account transfer service for cashless payment				

* The option for (ii) 1. includes a case where the organization's security policy is not satisfied (some policies are not followed) but the organization confirms that alternative measures, etc. are taken appropriately.

[Q42] Choose all applicable(*1) regarding safety measures against cloud services.
In Question 41, if you chose "2: No" for "7. Cloud service providers" in "(i) Whether there is any applicable organization," you do not need to answer to this question.
Note: This question is common to the FISC questionnaire survey. Please see "Common questions with FY2022 FISC questionnaire survey" on page 1.

Safety measures	Answer column (1: Yes; 2: No)
1. Establish an evaluation process at the time of considering the introduction of services	
2. Clarify the boundaries of responsibilities and the handling at the time of terminating cloud services in a written agreement	
3. Clarify the cloud base(*2) subject to control when using cloud services for specified systems(*3) in a written agreement	
4. Clarify the location of operational data when using cloud services for specified systems in a written agreement	
5. Use check tools, etc. for detecting errors in settings of cloud services	
6. Develop a structure for checking matters concerning specification changes for cloud services	
7. Develop a structure for making contact with a cloud service provider in the event of any failure	
8. Check whether a cloud service provider is registered in the list for cloud services of the Information system Security Management and Assessment Program (ISMAP(*4))	
9. Check the status of the acquisition of ISO certificates (ISO27001, ISO27017, etc.)	
10. Use third party assurance reports (SOC2, assurance reports under the IT Committee Practical Guidelines No. 7, etc.)	
11. Conduct on-site audits of cloud service providers	
12. Deploy personnel with expertise	
13. Build an internal cross-organizational structure (CCoE(*5))	
14. Other (Write details in the free column.)	

*1 If your organization uses multiple cloud services, choose all that are applicable for any one of them.
*2 A base to make effective access to data
*3 Out of financial information systems, a system having serious externality (a system whose failure may exert a significant social impact that cannot be controlled by individual financial institutions, etc. and a system containing sensitive information (including sensitive personal information) (a system that may cause broad damage to customers in the event of leakage of subtle information (including sensitive personal information), etc.)
*4 ISMAP (Information system Security Management and Assessment Program)
*5 CCoE (Cloud Center of Excellence)

If you chose "1: Yes" for "14. Other," please write details in the free column below.

This is the end of the questions for this self-assessment. If there is any challenge that you are aware of in developing and strengthening cybersecurity framework, please write details in the free column below.

(Examples of description)
- We are unable to fully understand the latest problems regarding cybersecurity.
- We would like to assign staff who can conduct incident analysis, etc. internally so as to ensure prompt responses when recognizing an incident, but we have no such staff.
- We have introduced a risk control product, but do not have staff who can understand the specification, etc. thereof, and are unable to understand threats that cannot be addressed with that product.
- It is difficult to properly evaluate cost-effectiveness when considering risk control measures (products, etc.), and the introduction is delayed.
- We consider zero day malware as a threat and would like to introduce a tougher mechanism to cope with, but we are unable to secure sufficient budget for that purpose.
- We would like to make a transition to public cloud services, but cannot promote the transition due to difficulties in conducting a risk assessment.
- We are enhancing cybersecurity frameworks, but are aware of the insufficiency in measures for certain things at present. We will strengthen them from now on.

[Free column]