(Appendix)

CSSA Check Sheet (FY2023)

Involvement of executives concerning cybersecurity

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

1. Have set up a management policy to ensure cybersecurity with the involvement of the chief executive (president, CEO, etc.) and have externally published it upon information disclosure or on a website, etc.
2. Have set up a management policy to ensure cybersecurity with the involvement of the chief executive (president, CEO, etc.) (not externally published)
3. Planning to set up a management policy to ensure cybersecurity
4. Have no plan to set up a management policy to ensure cybersecurity

Answer column (Choose one from 1. through 4.)

[Q2] Choose the applicable one regarding your organization's management plans concerning cybersecurity.

1. Have formulated a multiple-year management plan (in addition to a single-year one) concerning cybersecurity
2. Have formulated a single-year management plan concerning cybersecurity
3. Planning to formulate a management plan concerning cybersecurity
4. Have no plan to formulate a management plan concerning cybersecurity

Answer column (Choose one from 1. through 4.)

[Q3] Choose the applicable one regarding personnel in charge of cybersecurity at your organization.

1. An executive(*) solely in charge of cybersecurity (CISO, etc.)
2. An executive who administers the department in charge of managing system risks (including cybersecurity)
3. An executive who administers the department controlling risks
4. An executive who administers departments other than the department in charge of managing system risks (including cybersecurity) and the department controlling risks
5. Multiple executives (in charge of the cybersecurity affairs within the scope under their administration)
6. Staff of the department in charge of managing system risks (including cybersecurity) (other than an executive)
7. Staff of the department controlling risks (other than an executive)
8. Staff of departments other than the department in charge of managing system risks (including cybersecurity) and the department controlling risks (other than an executive)
9. No personnel in charge of cybersecurity

Answer column (Choose one from 1. through 9.)

* An executive includes an executive officer or an other staff with executive positions.

[Q4] Choose all applicable regarding the contents concerning cybersecurity that are periodically reported to your organization's personnel in charge of cybersecurity and to the chief executive (president, CEO, etc.) that you chose in Q.3.

Contents periodically reported	To personnel in charge of cybersecurity (Circle when applicable.)	To the chief executive (president, CEO, etc.) (Circle when applicable.)
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 that may affect the organization's systems		
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 staff members		
10. Other (Write details in the free column.)		
11. Periodic reports concerning cybersecurity are not made.		

If you chose "10. Other" for the contents periodically reported to the personnel in charge of cyber security, please write details in the free column below.

If you chose "10. Other" for the contents periodically reported to the chief executive (president, CEO, etc.), please write details in the free column below.

[Q5] Choose all applicable regarding the contents concerning cybersecurity that are reported on an ad-hoc basis to your organization's personnel in charge of cybersecurity and to the chief executive (president, CEO, etc.) that you chose in Q.3.

Contents reported on an ad-hoc basis	To personnel in charge of cybersecurity (Circle when applicable.)	To the chief executive (president, CEO, etc.) (Circle when applicable.)
1. Serious incidents that occurred in the organization's systems		
2. Serious incidents that occurred at other companies and may affect the organization		
3. A serious vulnerability (including inappropriate design or settings) that is found to affect the organization's systems		
4. Other (Write details in the free column.)		
5. Reports are not made on an ad-hoc basis.		

If you chose "10. Other" for the contents periodically reported to the personnel in charge of cyber security, please write details in the free column below.

If you chose "10. Other" for the contents periodically reported to the chief executive (president, CEO, etc.), please write details in the free column below.

Identifying and responding to risks concerning cybersecurity

[Q6] Choose all applicable regarding accidents, etc. due to cyberattacks to your organization.
Note: This question is common to the FISC questionnaire survey.

Details of the accidents, etc.	Answer column (Circle when applicable.)
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. Emergence of a fraudulent website or SNS using the organization's name	
8. Damage to the organization caused by a cyberattack to an outsourcee or external company	
9. Damage other than the above due to infection by a computer virus, etc.	
10. Other	
11. There has been no accident, etc.	

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

[Q7] Choose all applicable regarding collection of cybersecurity-related information.
Note: This question is common to the FISC questionnaire survey.

Information source	Answer column (Circle when applicable.)
1. From the FISC's "Cybersecurity Incident Information"	
2. From prefectural polices	
3. From the National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	
4. From the Financials ISAC Japan	
5. From bodies that collaborate diversely for responding to cyberattacks(*1)	
6. From companies to which the organization outsources cyberattack monitoring, and system integrators, security vendors, etc.	
7. By using threat intelligence services,(*2) etc.	
8. By attending various seminars	
9. From the internet (websites, SNS, etc.) or from the mass media, newspaper, etc.	
10. From group companies	
11. From industry associations and relevant industry organs	
12. From other sources	
13. Do not conduct information collection activities	

*1 Bodies that collaborate diversely for responding to cyberattacks refer to 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 "12. From other sources," please write details in the free column below.

[Q8] Choose the applicable one regarding the status of conducting an analysis and assessment of risks of cyberattacks.
Note: This question is common to the FISC questionnaire survey.

	Answer column (Choose one from 1. through 4.)
1. Considering cyberattacks to be risks and conducting a risk analysis and assessment periodically and as needed	
2. Considering cyberattacks to be risks and conducting a risk analysis and assessment periodically	
3. Considering cyberattacks to be risks and conducting a risk analysis and assessment as needed	
4. Do not conduct a risk analysis and assessment in relation to cyberattacks	

[Q9] (A question only for respondents who chose any of 1. through 3. in [Q8])
Choose all applicable regarding guidelines, frameworks, etc. you refer to when conducting a risk analysis and assessment.
Note: This question is common to the FISC questionnaire survey.

Status of making reference	Answer column (Circle when applicable.)
1. FISC's "Security Guidelines on Computer Systems for Banking and Related Financial Institutions"	
2. Ministry of Economy, Trade and Industry's "Cybersecurity Management Guidelines for Japanese Enterprise Executives"	
3. IPA's "Information Security Measures Guidelines for SMEs"	
4. NISC's "Risk Assessment Manual Based on the Idea of Guaranteeing Functions of Material Infrastructure"	
5. ISMS's "ISO/IEC 27001 (JIS Q 27001)"	
6. PCI SSC's "PCI DDS"	
7. NIST's "Cybersecurity Framework"	
8. FFIEC's "Cybersecurity Assessment Tool (CAT)"	
9. CIS's "CIS Controls"	
10. Cyber Risk Institute's "The Profile" (formerly, FSSCC's "Cybersecurity Profile")	
11. US MITRE's "ATT& CK"	
12. Ministry of Internal Affairs and Communications' "Teleworking Security Guidelines"	
13. Other guidelines or frameworks (Write details in the free column.)	
14. There are no guidelines or frameworks to refer to.	

If you chose "13. Other guidelines or frameworks," please write details in the free column below.

[Q10] 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.

Note: Provide an answer from the perspective of <u>conducting a risk assessment for material systems</u>.

Measures	Answer column (Circle when applicable.)
1. Conduct a risk assessment when introducing a new system or conducting a large-scale renewal	
2. Regularly conduct a risk assessment	
3. Conduct a risk assessment on an ad-hoc basis (each time an increase in cybersecurity risks is recognized)	
4. Conduct a risk assessment on an irregular base without specifying a timing	
5. Do not conduct a risk assessment	

[Q11] (A question only for respondents who chose any of 1. through 4. in [Q10])
Choose all applicable regarding the body that conducts a risk assessment concerning cybersecurity.

Body that conducts a risk assessment	Answer column (Circle when applicable.)
1. The department in charge of managing system risks (including cybersecurity)	
2. The department controlling risks	
3. A third-party professional organization (an outside vendor, consultant, etc.)	
4. The department in charge of systems	
5. Other	

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

[Q12] 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.
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 controlling risks.
4. 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 systems.
5. Responses (reduction, avoidance, transfer, or acceptance) based on the results of risk assessments are not made.

Answer column (Choose one from 1. through 5.)

Audits concerning cybersecurity

[Q13] Choose all applicable regarding the subjects of audits concerning cybersecurity and the status of conducting audits.

Audit subject	Status of conducting an audit (1: Conduct within the subject fiscal year(*1) / 2: Have conducted before but do not conduct within the subject fiscal year / 3: Have never conducted)	
	1. Verification by internal personnel(*2) (internal audit department)	2. Verification by an external (third-party) body(*2)
1. Appropriateness of executives' involvement		
2. Appropriateness of compliance with related laws and regulations and rules		
3. Appropriateness of the structure and budgets concerning cybersecurity		
4. Appropriateness of risk assessments		
5. Appropriateness of technical measures for material systems		
6. Status of compliance with rules and procedures concerning security measures		

*1 The subject fiscal year refers to one year from April 1, 2022 to March 31, 2023.
*2 Internal personnel (internal audit department) includes a holding company, etc. An external (third-party) body refers to an audit corporation, a consulting company, etc.

[Q14] 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 (Circle when applicable.)
1. Board of directors, governing board	
2. Audit committee	
3. Management council	
4. President, CEO, etc.	
5. Board of company auditors (company auditor), board of inspectors (inspector)	
6. Other (Write details in the free column.)	
7. The results are reported only to audited departments.	

If you chose "6. Other," please write details in the free column below.

[Q15] 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

[Q16] Choose the applicable one from 1. through 4. in the above box respectively for items 1. through 11. regarding the status of calling attention to and providing education and training concerning cybersecurity. You may choose "4. No applicable target" for items, "8. Provide education and training concerning cybersecurity targeting group companies and overseas offices" and "9. Check the status of outsourcees' implementation of training, etc."

1. Conduct within the subject fiscal year(*)
2. Have conducted before but do not conduct within the subject fiscal year
3. Have never conducted
4. No applicable target

Status of calling attention and providing education and training	Answer column (Choose one from 1. through 4. above.)
1. Occasionally issue warning statements to executives and staff members upon occurrence of an incident in and outside Japan	
2. Occasionally issue warning statements to executives and staff members and outsourcees when detecting a vulnerability	
3. Regularly provide all executives and staff members with classroom training and e-leaning (including learning using videos and documents, etc.) for awareness-raising	
4. Provide all executives and staff members with training against targeted emails	
5. Provide training for making responses with the assumption of cyber incident scenarios	
6. Provide education and training concerning cybersecurity only targeting executives	
7. Provide training on external disclosure targeting the PR department, etc. with the assumption of incident responses	
8. Provide education and training concerning cybersecurity targeting group companies and overseas bases	
9. Check the status of outsourcees' implementation of training, etc.	
10. Participate in exercises held by external organizations (FSA, Financials ISAC Japan, NISC, etc.)	
11. Other (If you chose 1. or 2., write details in the free column below.)	

* The subject fiscal year refers to one year from April 1, 2022 to March 31, 2023.

If you chose 1. or 2. in "11. Other," please write details in the free column below.

Securing and fostering of cybersecurity human resources

[Q17] Choose the applicable one from 1. through 4. in the above box respectively for items 1. through 8. regarding the status of securing cybersecurity human resources.

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

Status of securing human resources	Answer column (Choose one from 1. through 4. above.)
1. Human resources who assess cybersecurity risks associated with the introduction of new digital technologies	
2. Human resources who design and formulate cybersecurity strategies and plans	
3. Human resources who provide training and foster human resources regarding cybersecurity	
4. Human resources who design and develop systems from the perspective of cybersecurity	
5. Human resources who collect information on cybersecurity threats and vulnerability, and take measures against a vulnerability in systems	
6. Human resources who conduct log management and monitoring	
7. Human resources who make responses in the event of a cyber incident	
8. Human resources who conduct audits concerning cybersecurity	

[Q18] Choose all applicable regarding your organization's efforts for securing cybersecurity human resources.

Efforts for securing human resources	Answer column (Circle when applicable.)
1. Strengthen recruitment of new graduates	
2. Recruit mid-career workers via the website	
3. Recruit mid-career workers through scouting by the use of agent services or through referral based on a human network	
4. Transfer from group companies	
5. Accept employees on temporary assignment from friendly companies (a vendor, audit corporation, etc.)	
6. Other (Write details in the free column.)	
7. Do not make efforts to secure cybersecurity human resources in the organization	

If you chose "6. Other," please write details in the free column below.

[Q19] Choose all applicable regarding your organization's efforts for fostering cybersecurity human resources

Efforts for fostering human resources	Answer column (Circle when applicable.)
1. Formulate a plan for fostering cybersecurity human resources	
2. Implement personnel rotations with the aim of fostering cybersecurity human resources (long-term appointment)	
3. Temporarily transfer staff members to security vendors, system vendors, external organizations, etc.	
4. Hold internal lecture classes and study sessions	
5. Encourage staff members to participate in activities of the Financials ISAC Japan (working groups and exercises, etc.)	
6. Encourage staff members to participate in external training sessions or seminars (Expenses are borne by the organization.)	
7. Encourage staff members to obtain cybersecurity-related qualifications (Expenses for examinations and for qualification renewals are borne by the organization.)	
8. Do reskilling in a planned manner	
9. Other (Write details in the free column.)	
10. Do not make any efforts for fostering cybersecurity human resources	

If you chose "9. Other," please write details in the free column below.

Evaluation of digital technologies

[Q20] Choose the applicable one from 1. through 4. in the above box respectively for items 1. through 6. regarding the introduction of digital technologies and the matters you recognize as a cybersecurity threat associated with the introduction.

1. Have introduced digital technologies and are taking measures against recognized threats
2. Have introduced digital technologies and recognize threats but are not taking any measures
3. Have introduced digital technologies but recognize no threats
4. Have not introduced digital technologies

Cybersecurity threat associated with the introduction of digital technologies	Answer column (Choose one from 1. through 4. above.)
1. Information leakage due to defects in setting for public cloud services	
2. Illegal use of privileged accounts of public cloud services	
3. Falsification, outage, and information leakage due to unauthorized access to Open APIs (Write) from outside	
4. Information leakage from Open APIs (Read)	
5. Information leakage from smartphones and tablets	
6. Falsification, outage, and information leakage due to unauthorized access to a system for teleworking from outside	

Asset management

[Q21] 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 organization (including a case of outsourcing system operations). External systems are systems operated outside the organization (including cloud services, such as IaaS, PaaS, SaaS).

1. Have prepared a register, etc. and reflect changes automatically using an IT asset management tool, etc.
2. Have prepared a register, etc. and update them each time there is any change, and regularly check the content of the register
3. Have prepared a register, etc. and update them each time there is any change
4. Have prepared a register, etc. and regularly check the content of the register
5. Have prepared a register, etc. and irregularly check the content of the register
6. Have prepared a register, etc. but have not updated them
7. Have not prepared a register, etc.

(i) Internal systems: Answer column (Choose one from 1. through 7.)

(ii) External systems: Answer column (Choose one from 1. through 7.)

[Q22] 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 reflect changes automatically using an IT asset management tool, etc.
2. Have prepared a register, etc. and update them each time there is any change, and regularly check the content of the register
3. Have prepared a register, etc. and update them each time there is any change
4. Have prepared a register, etc. and regularly check the content of the register
5. Have prepared a register, etc. and irregularly check the content of the register
6. Have prepared a register, etc. but have not updated them
7. Have not prepared a register, etc.

(i) Hardware: Answer column (Choose one from 1. through 7.)

(ii) Software: Answer column (Choose one from 1. through 7.)

[Q23] (A question only for respondents who chose any of 1. through 6. in [Q22])
Choose all applicable regarding the information you are managing in a register, etc.

	Answer column (Circle when applicable.)	
Managed information	(i) Hardware	(ii) Software
1. Name		
2. Manufacturer		
3. Model number		
4. Serial number		
5. Firmware		
6. License number		
7. Version (including OS)		
8. Where to install (including the cloud)		
9. Maintenance/Support service period		
10. Names of departments and staff members using the software/hardware		

[Q24] 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 (Choose one from 1. through 6.)
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

[Q25] Choose the applicable one from 1. through 3. in the above box respectively for items 1. through 4. regarding the granting of accounts and access rights to material systems.
* Material systems are systems that an organization recognizes as especially important in its business operations, such as accounting systems and systems handling customer information.

1. Have formulated rules and procedures and are conducting monitoring
2. Have formulated rules and procedures
3. Have not formulated rules and procedures

Measures	Answer column (Choose one from 1. through 3. above.)
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 the highest access rights (privileged accounts) 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	

[Q26] Choose all applicable regarding the control of remote access to material systems.
* 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 (Circle when applicable.)
1. As operational management when making remote access (logging in) to material systems from outside, check and restrict 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 mobile equipment for remote connections or their authentication device (access token, IC card, etc.) that is necessary for identity verification upon making an access	
5. Restrict material systems that allow remote access	
6. Restrict applications for material systems that allow remote access	
7. Are allowing remote access but do not take any of the measures mentioned 1. through 6.	
8. Are not allowing remote access	

Data protection

[Q27] Choose the applicable one from 1. through 3. in the above box respectively for items 1. through 5. regarding measures for data protection.

1. Have formulated rules and procedures and are conducting monitoring
2. Have formulated rules and procedures
3. Have not formulated rules and procedures

Measures	Answer column (Choose one from 1. through 3. above.)
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 devices	
5. Using a means to automatically encrypt data (online storage, file transmission services, etc.) 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.

[Q28] Choose the applicable one from 1. through 3. in the above box respectively for items 1. through 4 regarding measures with the assumption that data in a material system are destroyed due to infection by ransomware, etc.
* Material systems are systems that an organization recognizes as especially important in its business operations, such as accounting systems and systems handling customer information.

1. Have formulated rules and procedures and are conducting monitoring
2. Have formulated rules and procedures
3. Have not formulated rules and procedures

Measures	Answer column (Choose one from 1. through 3. above.)
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. Regularly conduct recovery testing from backup data	

Log management

[Q29] Choose the applicable one from 1. through 3. in the above box respectively for items 1. through 4 regarding rules concerning audit trails (logs) for material systems.

* Material systems are systems that an organization recognizes as especially important in its business operations, such as accounting systems and systems handling customer information.

1. Have formulated rules and procedures and are conducting monitoring
2. Have formulated rules and procedures
3. Have not formulated rules and procedures

Measures	Answer column (Choose one from 1. through 3. above.)
1. Specification of logs to be obtained	
2. Storage period for logs	
3. Prohibition of unauthorized alteration and deletion of logs	
4. Operation to check any misconduct through periodic confirmation of logs	

Vulnerability management

[Q30] Choose the applicable one from 1. through 6. in the above box respectively for items 1. through 3. 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 renewa
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 (Choose one from 1. through 6. above.)	
Subjects	Vulnerability assessment (Web application)	Vulnerability assessment (platform)
1. Office automation environment(*)		
2. Website (website open to customers)		
3. 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.)

[Q31] Choose the applicable one from 1. through 6. in the above box regarding the timing of conducting a vulnerability assessment or otherwise inspecting the effectiveness of measures against attacks to mobile applications(*1) (when outsourcing system operations, including a case where you check the outsourcees' implementation of an assessment, etc.), respectively for DAST(*2) and SAST.(*3)
If you do not provide a mobile application, please choose "6. Do not provide a mobile application" for both.
*1 A mobile application is an application that operates on a mobile device such as a smartphone or tablet.
*2 Dynamic Application Security Testing (DAST) is conducted for programs and software products in an action state.
*3 Static Application Security Testing (SAST) is conducted based on programs' source codes.

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 a mobile application

	By type (Choose one from 1. through 6. above.)	
Subject	DAST (Mobile application)	SAST (Mobile application)
1. Mobile application		

[Q32] Choose the applicable one from 1. through 5. in the above box respectively for items 1. and 2. regarding the status of having conducted penetration testing(*1) and threat-led penetration testing.(*2) (Please answer regarding testing you have conducted up until March 31, 2023 (including testing you conducted prior to March 2022).)

*1 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 such means as using simulated malware or abusing a vulnerability or a defect in settings.

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

Test typ	Answer column (Choose one from 1. through 5. above.)
1. Penetration testing	
2. Threat-led penetration testing, etc.	

[Q33] Choose the applicable one from 1. through 6. in the above box respectively for items 1. and 2. regarding policies for applying a patch when a serious vulnerability is found in your organization's systems.

1. Apply a patch promptly
2. Apply a patch by specifying a certain period for making responses
3. Apply a patch at a timing of maintenance, etc.
4. Apply a patch at the time of renewal of systems
5. Do not apply a patch in principle
6. Have no policies concerning the application of a patch

Systems and terminals	Answer column (Choose one from 1. through 6. above.)
1. Systems and terminals connected to the internet(*)	
2. Systems and terminals unconnected to the internet	

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

[Q34] Choose all applicable regarding the criteria for deciding on the application of a patch against a serious vulnerability.

Criteria	Answer column (Circle when applicable.)
1. Indices specified by the CVSS or other external information providers	
2. Warnings issued by the authority or the Financials ISAC Japan	
3. Information recommended by system vendors	
4. System characteristics (significance of the system, information the system handles, whether the system is connected to the internet, etc.)	
5. Whether the attack code is disclosed	
6. Whether there is any information on an attack	
7. Individual judgments made by internal experts	
8. Other (Write details in the free column.)	
9. There are no criteria.	

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

[Q35] 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.
* Material systems are systems that an organization recognizes as especially important in its business operations, such as accounting systems and systems handling customer information.

	Answer column (Choose one from 1. through 4.)
1. The executive 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

[Q36] 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 (Circle when applicable.)
1. Separate the network of OA terminals and the internet (including separation by physical means and by the use of a virtual browser or other logical means)	
2. Separate the environment to execute Web content to be displayed on a terminal browser (such as the introduction of a CDR solution)	
3. Restrict websites that can be accessed from OA terminals	
4. 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)	
5. Have introduced a signature-based anti-malware product to OA terminals	
6. Have introduced a behavior-based anti-malware product (including EDR) to OA terminals	
7. Restrict connections of external storage devices to OA terminals	
8. Have restricted access points to connect OA terminals in advance (restrict unauthorized wireless communications, etc.)	
9. Have introduced a mechanism of multi-factor authentication for logging in to OA terminals	
10. Conducting none of 1. through 9. above	

[Q37] Choose all applicable regarding measures against cyberattacks taken at the border between your organization and the outside.

Measures	Answer column (Circle when applicable.)
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. Identify devices that may become penetration routes, such as VPN and RDP, and take measures against a vulnerability concerning them	
7. Control access to the internet by the use of authentication function	
8. Conducting none of 1. through 7. above	

* 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.

[Q38] When you provide a website (website open to customers) or internet banking services, choose all applicable regarding measures against cyberattacks taken for each of them.

Measures	Answer column (Circle when applicable.)	
	Website (website open to customers)	Internet banking services
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.)		
7. Providing a website (website open to customers)/internet banking services, but conducting none of 1. through 6. above		
8. Not providing a website (website open to customers)/internet banking services		

* 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.

[Q39] If you provide a mobile application, choose any of 1: through 3: respectively in each column regarding security measures for the mobile application.

Security measures for the mobile application	Answer column (1: Yes / 2: No / 3: Do not provide a mobile application)
1. Measures to protect data transmitted and received	
2. Measures to protect data stored in terminals	
3. Restriction of the operations of OS for which the support service period has expired	
4. Adoption of a multi-factor authentication system	
5. Implementation of reverse engineering	
6. Collection of information on vulnerability regarding third-party products (other companies' products used for the mobile application and infrastructure for providing the mobile application)	
7. Use of a secure encryption method	
8. Detection of abnormal transactions	

[Q40] Choose any of 1: through 3: respectively in each column regarding the status of introducing or considering the introduction of other measures against cyberattacks.

Measures	Answer column (1: Have introduced / 2: Considering the introduction / 3: Have done nothing)
1. Introduction of a mechanism to limit the scope of activities of malware, etc. that have penetrated into the organization (including microsegmentation of the network)	
2. Introduction of a behavior-based anti-malware product (including EDR) to the organization's server	
3. Introduction of a mechanism to detect suspicious activities of users within the organization (including UEBA)	
4. Introduction of a mechanism to verify the security policy introduced to cloud services (including CASB)	
5. Introduction of a mechanism to centrally manage privileged IDs for internal systems and external systems (including PAM)	
6. Introduction of a solution to integrate security-related operations and automatize responses (including SOAR)	

Detection

[Q41] Choose the applicable one regarding a body that conducts monitoring and analyses of cybersecurity-related issues for material systems (such as SOC (including a case of outsourcing the monitoring and analyses)).
* Material systems are systems that an organization recognizes as especially important in its business operations, such as accounting systems and systems handling customer information.

	Answer column (Choose one from 1. through 4.)
1. Have established a body (monitoring and analyses are being conducted 24 hours a day, 365 days a year) 2. Have established a body (monitoring and analyses 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	

[Q42] (A question only for respondents who chose any of 1. through 3. in [Q41])
Choose all applicable regarding targets monitored by an SOC or other department that conducts monitoring and analyses of cybersecurity-related issues.

Targets for cybersecurity monitoring	Answer column (Circle when applicable.)
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 suspicious activities in the organization's internal network (suspicious operations of terminals and servers, nonconformity when conducting analyses by correlating various logs)	
11. Other (Write details in the free column.)	

If you chose "11. Other," please write details in the free column below.

Incident response and recovery

[Q43] Choose the applicable one regarding staff for making responses (including your parent company, etc.) upon a cyber incident.

	Answer column (Choose one from 1. through 3.)
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	

[Q44] Choose all applicable regarding the policy of offering cooperation (information provision) to industry associations, relevant industry organs, and external organizations (Financials ISAC Japan, etc.).

Policy of cooperation	Answer column (Circle when applicable.)
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. Make a decision as the necessity arises	
7. Do not provide information	
8. Other (Write details in the free column.)	
9. Have not formulated a policy	

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

[Q45] 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 (Circle when applicable.)
1. Have formulated the criteria for the prioritization in response policies (triage) for cyber incidents	
2. Have formulated rules and procedures to transfer the authority in the absence of personnel who make decisions and gives instructions and other responsible personnel	
3. Have formulated rules and procedures to separate systems from the relevant network promptly at the stage when infection by malware is suspected	
4. 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	
5. 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	
6. Have formulated rules and procedures to shut down systems based on the background of a cyber incident	
7. Have formulated rules and procedures for external disclosure upon a cyber incident	
8. Have formulated rules and procedures to continue business operations using alternative means upon system outage	
9. Have formulated the criteria for deciding on the resumption of system operations	
10. Have formulated rules and procedures for incident responses at night and on holidays	
11. Have formulated none of the rules and procedures 1. through 10. above	

[Q46] Choose the applicable one regarding the status of strengthening frameworks based on past responses to incidents (including training and exercises).

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 frameworks as necessary
3. In light of past responses to cyber incidents, update only technical measures as necessary
4. Do not update frameworks and technical measures in light of past responses to cyber incidents
5. Have no record of making responses to cyber incidents

Answer column (Choose one from 1. through 5.)

[Q47] Choose the applicable one respectively regarding the content of contingency plans by type of cyberattacks 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 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: Conduct within the subject fiscal year(*) / 2: Have conducted before but do not conduct within the subject fiscal vear / 3: Have never conducted)
5. Outsoucees also participate in training and exercises regarding contingency plans (1: Yes / 2: No / 3: No applicable target)

Cyberattacks	Whether having formulated contingency plans against attacks			Status of conducting training and exercises of contingency plans	
	1. (1: Yes / 2: No)	2. (1: Yes / 2: No)	3. (1: Yes / 2: No)	4. (Choose one from 1. through 3. above.)	5. (1: Yes / 2: No / 3: No applicable target)
1. Falsification of websites					
2. DDoS attacks					
3. Ransomware attacks					

* The subject fiscal year refers to one year from April 1, 2022 to March 31, 2023.

[Q48] Choose all applicable regarding the status of developing points of contact and the communication loop for reporting to the relevant parties upon the occurrence of a cyberattack (damage). You may choose "4: No applicable target" for items, "5. Outsourcees," "6. The organization's group companies," and "13. Other."

Target to report	Answer column (1: Procedures are documented and disseminated. / 2: Procedures are documented. / 3: Procedures are not documented / 4: No applicable target)
1. The organization's emergency contact network	
2. Ministries and agencies concerned, The Bank of Japan	
3. Industry associations and relevant industry organs	
4. Customers	
5. Outsourcees	
6. The organization's group companies	
7. Mass media and the press	
8. External organizations (Financials ISAC Japan, FISC, etc.)	
9. Organizations that accept reports on vulnerability and cyber incidents (IPA, JPCERT, etc.)	
10. Private companies specialized in cybersecurity	
11. Prefectural polices	
12. Personal Information Protection Commission	
13. Other (If you chose 1: or 2: here, write details in the free column below.)	

If you chose 1: or 2: in "13. Other," please write details in the free column below.

Management of third parties

[Q49] Choose all applicable respectively regarding the status of management and monitoring of cybersecurity for your organization, overseas bases, affiliated companies and third parties.(*1)

Organization	(i) Whether there is any applicable organization (1: Yes / 2: No) If you chose "2: No," you do not need provide answers in (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 (followed)(*4) 2. Recognize that the organization's security policy is not satisfied (some 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 (Circle when applicable.)	Use services that conduct evaluation, analyses and rating, etc. concerning applicable organizations' cybersecurity (Circle when applicable.)
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(*2) (Regarding cloud service providers, provide answers in 7.)				
6. Companies to which open APIs are connected				
7. Cloud service providers(*3)				
8. Businesses with which the organization collaborates on payment services, such as account transfer service for cashless payment				

*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 An outsourcee is an organization to which the organization outsources its business operations (such as a vendor of a system (including a joint center, etc.) to which a financial institution outsources its business operations for providing financial services, including a case where the situation can be considered equivalent to outsourcing even without an outsourcing agreement concluded and a case where outsourced business operations are performed overseas).
Regarding cloud service providers, provide an answer in the answer column for cloud service providers.

*3 A cloud service provider is a provider of IaaS, PaaS, or SaaS.

*4 "1. Confirm that the organization's security policy is satisfied (followed)" of (ii) includes a case where the organization's security policy is not satisfied (some are not followed) but it is confirmed that alternate measures, etc. are properly taken.

[Q50] Choose all applicable 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 (Choose one from 1. through 4.)
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. 4. No applicable important third party	

[Q51] (A question only for respondents who chose any of 1. through 3. in [Q50])

Choose all applicable regarding the status of conducting a risk assessment concerning cybersecurity when and after selecting an important third party.(*1) Provide an answer in each of the answer columns for outsoucees,(*2) cloud service providers,(*3) and third parties excluding outsourcees and cloud service providers.(*4)

In Q49, if you chose "2: No" in "5. Outsourcees," you do not need to provide answers regarding outsourcees. If you chose "2: No" in "7. Cloud service providers," you do not need to provide answers regarding cloud service providers.

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

*2 An outsourcee is an organization to which the organization outsources its business operations (such as a vendor of a system (including a joint center, etc.) to which a financial institution outsources its business operations for providing financial services, including a case where the situation can be considered equivalent to outsourcing even without an outsourcing agreement concluded and a case where outsourced business operations are performed overseas).
Regarding cloud service providers, provide an answer in the answer column for cloud service providers.

*3 A cloud service provider is a provider of IaaS, PaaS, or SaaS.

*4 Third parties excluding outsourcees and cloud service providers are third parties other than those mentioned in *2 and *3 above (ex. an electronic payment service provider or a fund transfer service provider in a business partnership).

	Status of conducting a risk assessment	Answer column for outsourcees (Circle when applicable.)	Answer column for cloud service providers (Circle when applicable.)	Answer column for third parties excluding outsourcees and cloud service providers (Circle when applicable.)
When selecting an important third party	1. Conduct a risk assessment based on documents			
	2. Conduct a risk assessment through hearings			
	3. Conduct a risk assessment through visual confirmation, such as an on-site investigation			
	4. Conduct a risk assessment by using an external risk assessment service provider			
	5. Conduct none of 1. through 4. above			
	6. No applicable important third party			
After selecting an important third party	7. Regularly conduct a risk assessment based on documents			
	8. Regularly conduct a risk assessment through hearing			
	9. Regularly conduct a risk assessment through visual confirmation, such as an on-site investigation			
	10. Regularly conduct a risk assessment by using an external risk assessment service provider			
	11. Conduct none of 7. through 10. above regularly			
	12. No applicable important third party			

[Q52] Choose all matters that are prescribed from the perspective of cybersecurity in agreements, etc. with third parties.
Provide an answer in each of the answer columns for agreements, etc. with outsourcees and agreements, etc. with third parties excluding outsourcees and cloud service providers. Regarding cloud service providers, please answer Q53.
In Q49, if you chose "2: No" in "5. Outsourcees," you do not need to provide answers regarding outsourcees.

Matters prescribed	Answer column for agreements, etc. with outsourcees (Circle when applicable.)	Answer column for agreements, etc. with third parties excluding outsourcees and cloud service providers (Circle when applicable.)
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. Implementation and reporting of vulnerability assessment for the system environment where outsourced operations are performed		
6. Responses and reporting when a serious vulnerability is found in the system environment where outsourced operations are performed		
7. Permission of the organization's on-site investigations		
8. Reporting to the organization when a third party recontracts with another third party for the outsourced operations that may affect the organization's cybersecurity		
9. Have prescribed none of 1. through 8. above		

[Q53] Choose all applicable(*1) regarding safety measures against cloud services.
In Question 49, if you chose "2: No" in "7. Cloud service providers" in "(i) Whether there is any applicable organization," you do not need to answer this question.

Note: This question is common to the FISC questionnaire survey.

Safety measures	Answer column (Circle when applicable.)
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(*5)	
12. Deploy personnel with expertise	
13. Build an internal cross-organizational structure (CCoE(*6))	
14. Other	
15. Conduct none of 1. through 14. above	

*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 sensitive information (including sensitive personal information), etc.)
*4 ISMAP (Information system Security Management and Assessment Program)
*5 If an on-site audit cannot be conducted due to restrictions on the side of a service provider, please leave the column blank.
*6 CCoE (Cloud Center of Excellence)

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

Measures against threats of illegal remittances and phishing attempts

[Q54] Choose all applicable regarding the status of taking measures against illegal remittances and phishing attempts.
If you do not provide internet banking services or a mobile application, please choose "4: Do not provide services" or "4: Do not provide a mobile application" in all of the relevant answer columns.

Measures against illegal remittances and phishing attempts	Answer column for internet banking services (1: Taking measures / 2: Considering measures / 3: Do not consider any measures / 4: Do not provide services)	Answer column for a mobile application (1: Taking measures / 2: Considering measures / 3: Do not consider any measures / 4: Do not provide a mobile application)
1. Issue warning statements to users (counterparties)		
2. Apply multifactor authentication at the time of login		
3. Apply multifactor authentication at the time of executing fund transfer		
4. Give notices on transaction status (login history, change of passwords, remittances, etc.) to users		
5. Provide security software		
6. Introduce Domain-based Message Authentication, Reporting, and Conformance (DMARC)		
7. Develop procedures for detecting phishing websites and taking them down		
8. Set up an emergency contact office		

Zero trust security

[Q55] Choose the applicable one regarding the status of introducing a zero trust architecture.
* Zero trust is the thinking concerning cybersecurity that places the focus on "protecting the organization's information assets and IT assets by constantly verifying the reliability of access instead of implicitly trusting access from the organization's networks and devices."
When answering to this question, please refer to the following:
"Report on the Survey of the Current Situation of the Introduction of a Zero Trust Architecture and the Case Analysis"
https://www.fsa.go.jp/common/about/research/20210630/zerotrust.pdf (Available only in Japanese)

	Answer column (Choose one from 1. through 7.)
1. Operating a zero trust architecture 2. Proceeding with the introduction and implementation of a zero trust architecture 3. Proceeding with the risk assessment and formulation of policies for introducing a zero trust architecture 4. Endeavoring to understand the current status for introducing a zero trust architecture 5. Considering the introduction of a zero trust architecture 6. Considered the introduction of a zero trust architecture and decided not to introduce 7. Do not consider the introduction of a zero trust architecture	

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]