API Connection Checklist (Format)
<October 2018 Edition>

October 12, 2018
Council of Experts on Open API for Financial Institutions
Working Group on API Connection Checklist for Financial Institutions

No.	Category	Security objectives	Subject party	Current status	Issues to be addressed	Improvement plans	Related rules	Part of related rules	Notes
1	Governance of information and security management	Make clear who is responsible for what regarding security management.	API connection partner				FISC Security Guidelines	C4, C6, C7, C8	
2	Governance of information and security management	Establish security management rules.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles --------- FISC Security Guidelines	3.3.1 Eligibility of Third Parties d --------- C1, C12	
3	Governance of information and security management	Establish firmly governance of security management through means including (1) ensuring that all executives and employees thoroughly understand information management methods and (2) doing follow-up monitoring.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles --------- FISC Security Guidelines	3.3.1 Eligibility of Third Parties d 3.3.3 Countermeasures for Internal Unauthorized Access e --------- C13, C14, A1	
4	Governance of information and security management	Manage information assets.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.3 Countermeasures for Internal Unauthorized Access e	
5	Governance of information and security management	Implement measures to prevent misconduct by executives and employees.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.3 Countermeasures for Internal Unauthorized Access c	
6	Governance of information and security management	Prevent leakage of information from devices and other equipment when the organization’s services are terminated or systems are disposed of.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.3 Countermeasures for Internal Unauthorized Access e	

No.	Category	Security objectives	Subject party	Current status	Issues to be addressed	Improvement plans	Related rules	Part of related rules	Notes
7	Governance of information and security management	Implement review and countermeasures in the event of a security incident.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.1 Eligibility of Third Parties b	
8	Governance of information and security management	Ensure security in chain connections.	API connection partner						
9	Governance of information and security management	Prepare for incidents such as unauthorized access and system failures.	Both				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.4 Handling Unauthorized Access When It Occurs c	
10	Outsourcing management	Implement measures as necessary to ensure effective and proper execution of outsourced operations.	API connection partner				FISC Security Guidelines	C20, C21, C22, C23, A1	
11	Outsourcing management	Implement measures in light of risks specific to cloud services when using them.	API connection partner				FISC Security Guidelines	C24, A1	
12	Cooperation between financial institutions and API connection partners	Review and improve security measures.	Both				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.4 Handling Unauthorized Access When It Occurs c	
13	Cooperation between financial institutions and API connection partners	Implement appropriate responses to requests, inquiries, and other contacts from users.	Both				JBA “Report of Review Committee on Open APIs” User Protection Principles	3.4.2 Explaining/Displaying Information and Obtaining Consent i, j	

API Connection Checklist (Format)
<October 2018 Edition>

No.	Category	Security objectives	Subject party	Current status	Issues to be addressed	Improvement plans	Related rules	Part of related rules	Notes
14	Cooperation between financial institutions and API connection partners	Prevent spread of damage to users.	Both				JBA “Report of Review Committee on Open APIs” User Protection Principles	3.4.4 Actively Preventing Incidence and Spread of Damages d	
15	Cooperation between financial institutions and API connection partners	Compensate users appropriately when needed.	Both				JBA “Report of Review Committee on Open APIs” User Protection Principles	3.4.5 Responsibilities Toward and Compensation of Users c	
16	Cooperation between financial institutions and API connection partners	Operate contact points for user compensation properly.	Both				JBA “Report of Review Committee on Open APIs” User Protection Principles	3.4.5 Responsibilities Toward and Compensation of Users d	
17	Management of computer facilities	Implement countermeasures against information leakage from computer facilities.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.3 Countermeasures for Internal Unauthorized Access e	
18	Management of office facilities	Prevent entry of unauthorized persons and restrict access to important information.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.3 Countermeasures for Internal Unauthorized Access e	
19	Management of office facilities	Prevent persons involved from taking information out of the premises.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles --------- FISC Security Guidelines	3.3.3 Countermeasures for Internal Unauthorized Access e -------- P49	
20	Management of office facilities	Prevent attacks such as intrusions to internal systems through infection with computer viruses.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access s	

API Connection Checklist (Format)
<October 2018 Edition>

No.	Category	Security objectives	Subject party	Current status	Issues to be addressed	Improvement plans	Related rules	Part of related rules	Notes
21	Management of system development and operations	Prevent unauthorized access to information assets from within.	API connection partner				JBA “Report of Review Committee on Open APIs” Security principle --------- FISC Security Guidelines	3.3.3 Countermeasures for Internal Unauthorized Access e --------- P27, P29	
22	Management of system development and operations	Implement authentication on system access.	API connection partner				FISC Security Guidelines	P1, P8, P16, P26	
23	Management of system development and operations	Maintain logs of access to and use of systems to enable investigation in the event of incidents.	API connection partner				FISC Security Guidelines	P10	
24	Management of system development and operations	Implement countermeasures to prevent misconduct by operators.	API connection partner						
25	Management of system development and operations	Implement measures as necessary to prevent marked deterioration in quality when making changes to systems.	API connection partner						
26	Management of system development and operations	Implement countermeasures against unauthorized access from the outside.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access x	
27	Management of system development and operations	Implement countermeasures against vulnerabilities in systems and networks.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access s	

API Connection Checklist (Format)
<October 2018 Edition>

No.	Category	Security objectives	Subject party	Current status	Issues to be addressed	Improvement plans	Related rules	Part of related rules	Notes
28	Management of system development and operations	Manage confidential information taken out of the premises.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.3 Countermeasures for Internal Unauthorized Access e	
29	Service-system security functions	Implement management measures suited to the types and contents of data.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access x	
30	Service-system security functions	Implement countermeasures against leakage of confidential information.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access s	
31	Service-system security functions	Enable restoration of lost or damaged information.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access s	
32	Service-system security functions	Develop authentication functions to protect users.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access m	
33	Service-system security functions	Implement countermeasures against fake applications.	API connection partner						
34	Service-system security functions	Keep the spread of damage from unauthorized access to a minimum.	Both				JBA “Report of Review Committee on Open APIs ” Security Principles	3.3.4 Handling Unauthorized Access When It Occurs a	

API Connection Checklist (Format)
<October 2018 Edition>

No.	Category	Security objectives	Subject party	Current status	Issues to be addressed	Improvement plans	Related rules	Part of related rules	Notes
35	Service-system security functions	Enable tracing in the event of unauthorized access.	Both				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access s 3.3.4 Handling Unauthorized Access When It Occurs b	
36	API security functions	Implement countermeasures against leakage of confidential information related to authentication and authorization.	API connection partner				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access g	
37	API security functions	Prevent unexpected usage of API.	API connection partner						
38	API security functions	Ensure that user accounts are not used to establish API connection without the user’s knowledge.	Financial institution				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access b	
39	API security functions	Realize the strength of authentication that strikes a suitable balance between user convenience and user protection suited to the risk involved.	Financial institution				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access c	
40	API security functions	Implement multilayered protection against attacks targeting vulnerabilities.	Financial institution				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access s	
41	API security functions	Reduce the risk of misuse of authentication as much as possible.	Financial institution				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access g, m	

API Connection Checklist (Format)
<October 2018 Edition>

No.	Category	Security objectives	Subject party	Current status	Issues to be addressed	Improvement plans	Related rules	Part of related rules	Notes
42	API security functions	Protect users through the overall strength of authentication, including the strength maintained by API connection partners.	Financial institution				JBA “Report of Review Committee on Open APIs” Security Principles	3.3.2 Countermeasures for External Unauthorized Access m	
43	Security of API use	Ensure accountability to users regarding their API use.	API connection partner				JBA “Report of Review Committee on Open APIs” User Protection Principles	3.4.2 Explaining/Displaying information and Obtaining Consent d	
44	Security of API use	Prevent user misconceptions and misunderstandings regarding API connections.	Financial institution				JBA “Report of Review Committee on Open APIs” User Protection Principles	3.4.2 Explaining/Displaying information and Obtaining Consent c	