Information Security Rating Summary

No. 18K0011
October 11, 2018
I.S.Rating Co., Ltd.

1． Rating Results

Company Name	BITPoint Japan Co., Ltd.
Rating Type	Information Security Rating
Rating ID Code	10000420101C1802
Rating Scope	Cryptocurrency exchange service (Total management, including acquisition, use, storage, transfer and erasure, of important information)
Rating Target	Departments in charge of operational management of cryptocurrency exchange service: Compliance Department, Marketing Department, System Management Department, Operations Department, Trading Department, Customer Service Department
Assumed Risk	Information leakage
Rating	Ais (single A flat)
Direction of Rating	Stable
Period of Validity	From October 11, 2018 to October 10, 2019 (One year from the date of issuance)

* The methods that we use for rating examination are interviewing responsible persons, looking through rules, ledgers and the like, and inspecting related facilities. With regard to security measures that are being planned and have therefore not yet been implemented, we check the design specifications using related documents. After the measures are implemented, we will check again as to whether the measures have been implemented according to the plan or not.

* This rating certifies that the situation on the date of on-site examination was verified, and does not guarantee that such situation exists all the time on a continual basis. We also recommend checking by conducting re-examination once a year in normal times, or as necessary in emergencies, according to changes in the specifications of the target of the rating or changes in the social environment.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

2. Reason for Assigning the Rating

BITPoint Japan Co., Ltd. engaged in cryptocurrency exchange service (Minato-ku, Tokyo; hereinafter, "BITPoint") is enhancing its management structure, with the goal of achieving safe and secure cryptocurrency trading. As announced in "Progress and Implementation of Management Structure Enhancement" disclosed on its website on September 21, 2018, BITPoint is radically enhancing its management structure with focus themes of information security management structure, cyber security management structure, user information management structure, and response to complaints, and taking specific measures including:

- Conducting penetration testing by a third-party organization on a regular basis
- Implementing multitiered information security measures that cover information security terminals in the office
- Building a system for identifying information security risks with the CISO to respond to risks in advance
- Building a comprehensive security structure that covers prevention of impropriety
- Establishing a call center in Okinawa to handle complaints

We determined that the scope should be the total management, including acquisition, use, storage, transfer and erasure, of important information in cryptocurrency exchange service, and reviewed the status of initiatives taken by departments in charge of operational management of cryptocurrency exchange service from the perspectives of management maturity and security strength.

In terms of management maturity, BITPoint has developed the Information Security Policy, established the Information Security Committee, assigned a Chief Information Security Officer (CISO), as well as staff responsible for information management at all departments, and built an organizational structure on both top-down and bottom-up bases. Particularly with regard to risk assessment, BITPoint has analyzed and evaluated each attack scenario with a focus on the most important target of "theft of users' cryptocurrency," and set and managed goals, including taking initiatives for reducing risk value in a planned manner.

In terms of security strength, BITPoint has been performing monitoring and control using management

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

tools for preventing unauthorized access and information leakage based on the results of the earlier-mentioned risk assessment. Specifically, the company is implementing measures against cyberattack threats, such as a function of diverting access to the production server machine and inspecting vulnerability through penetration testing by white hat hackers. BITPoint also incorporates (heuristic, deterrent, preventive) control measures against malicious outsiders, which include a 24 hours a day, every day monitoring system that can detect abnormalities.

On the whole, in terms of both management maturity and security strength, BITPoint is implementing measures that exceed the initiatives required for general enterprises' business transactions and satisfying a certain level needed for handling of financial and securities information. From the perspective of management maturity, it is desirable that BITPoint should own processes for continual improvement and maintain and develop the high-level management status in the future so that the company can respond to environmental changes as its business moves toward the growth period as well as to cyberattack threats that change from day to day. From the security strength perspective, it is desirable to step up measures against malicious outsiders, incorporate enhancement of control measures, including constant monitoring of malicious insiders, and implement measures in stages by considering their priority.

3. Confirmation Results

(1) Management Policy

BITPoint has set its corporate mission of providing customers and society with safe, secure, comfortable, convenient, and high-quality online cryptocurrency trading, as well as its management policy of taking actions with a socially sensible manner. To achieve the management policy, the company considers information security measures and management of customers' assets, including personal information, as one of the most important tasks, and declares on its website that it is making proactive efforts to help build a safe and secure cryptocurrency exchange industry.

(2) Information Security Initiatives

Recognizing that its management of information required for cryptocurrency exchange service is an important management issue for living up to customers' expectations and ensuring lasting growth of the company, BITPoint has been proactively working on information security management, including the following:

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

- Developed the Information Security Policy, which is based on systematic security control measures, human security control measures and technical security control measures, to ensure appropriateness in managing customer information assets, and built an information security system, which is led by the management, to put in place a system to maintain and improve information security.
- Established the Information Security Committee with the president as the person with ultimate responsibility for information security, appointed an executive officer in charge of information security as the committee's chairperson, and established the Secretariat of the Information Security Committee and a department in charge of cyber measures (System Management Department) to implement measures for preventing information leakage.
- Established a call center, which put in place measures at the information security level required for a financial institution, to provide customer service over the phone. The center has a support system that allows even a customer who engages in cryptocurrency trading for the first time to conduct trading with a sense of security.

（3）Matters Confirmed as to Information Security Measures

In carrying out operations for cryptocurrency exchange service, BITPoint refers to the Information Security Policy, as well as the operational instructions of security control measures of the Guidelines on Personal Information Protection in the Financial Field, which is provided by the Financial Services Agency and the Personal Information Protection Commission, and the Guidelines for Administrative Processes Vol. 3 (Virtual Currency Exchange Companies), and I.S.Rating confirms the following. It has also been confirmed, in particular, that BITPoint's trading system was developed by members who developed a major online securities system, and that the development team having an understanding of financial systems made efforts to achieve the robust security required for securities companies.

I. Development of the basic policy
II. Development of handling standards
III. Systematic security control measures
IV. Human security control measures
V. Technical security control measures
VI. Priority security measures

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

Information Security Rating Summary

Item No.	Item	Measures implemented
I. Development of basic policy		
1	Developing basic policy	・As a way to cover the cryptocurrency exchange service protection policy, the Information Security Policy provides the basic information security policy, name of business operator, compliance with related laws, regulations, and guidelines, information security rules related to security control measures, and various standards related information security. The Information Security Policy sets the flow outlining response to information security incidents and accidents as specific standards for information handling, standards for information system use, standards for information system management, standards for physical measures, and standards for information security incident/accident response, and clarifies the responses that officers and employees should make.
II. Development of handling standards		
1	Developing handling standards	・The Standards for Information Handling in the Information Security Policy provide detailed rules about information handling in cryptocurrency exchange service. The standards stipulate security control measures with regard to paper media and electronic data handling required for officers and employees in the stages of information acquisition, use, storage, transfer and erasure.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

Information Security Rating Summary

III. Systematic security control measures		
1	Appointing persons responsible for data management	・The president is designated as the person with ultimate responsibility for information security (Information Security Rules Article 4). ・The president has appointed an executive officer in charge of information security, from among the officers and employees, as the Information Security Committee Chairperson. ・The Information Security Committee Chairperson has appointed information security committee members, and held information security committee meetings every month. The committee has a mechanism for enhancing its checking function and ensuring governance to promote information security management, which includes discussing the basic policy and important matters related to information security (Information Security Rules Article 5). ・The Information Asset Management Ledger has been created to specify the persons in charge of management, scope of users, storage location, level of importance, and possible risks by type of information, and reviewed on a regular basis.
2	Specifying security control measures in the work regulations, etc.	・Security control measures are stipulated in the Information Security Rules, standards related to information security, etc. ・It is stipulated that anyone who has violated the rules and standards and neglected efforts for improvement or anyone who has intentionally committed a violation will be subject to disciplinary action according to the work regulations.
3	Operations in accordance with handling rules related to data security control	・Standards for Information Handling have been set to stipulate categories of information, management and handling of information, use of portable media, handling of personal information, etc. ・Identification procedure in which personal information is handled is performed in an area differentiated as a security area as stipulated in the Standards for Physical Measures.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

4	Specifying means of confirming status of data handling	・All personal computers (PCs) involved in cryptocurrency exchange service are equipped with an integrated log management tool and monitored. Handling of portable media is restricted, and records of the use of the PCs (login history, access log, etc.) are acquired and stored.
5	Developing and implementing a system for data handling inspection and audit	・An audit system has been put in place for inspection and audit of all departments involved in cryptocurrency exchange service. A future audit plan has been developed and is being implemented in stages.
6	Developing a system for responding to information leakage, etc.	・There is a 24 hours a day, every day monitoring system that can issue an alert in the event of an abnormality, such as unauthorized access or when information is taken out unlawfully, and promptly detect the abnormality. ・A system for reporting information security problems, if they occur during clerical work for cryptocurrency exchange service, in accordance with the Standards for Information Security Incident/Accident Response has been built. ・There is a system that enables the Information Security Committee Chairperson to promptly and properly provide explanation to customers affected, report to the authority, and disclose information as necessary in the event of an information security problem (Standards for Information Security Incident/Accident Response 4 (3)).
IV. Human security control measures		
1	Concluding data nondisclosure agreement with employees	・All officers and employees have agreed, signed, and affixed their seal on the letter of consent on the Information Security Policy and submitted the letter to the company. Issues covered in the letter include nondisclosure agreement and punishment for violations (Information Security Rules Article 19).
2	Clarifying roles and responsibilities of employees	・The Rules on Division of Duties have been set to clarify roles and responsibilities of each department.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

3	Employee awareness raising, education and training on security control measures	・The staff in charge of education, who have been appointed by the Information Security Committee Chairperson, provide new hires with training on an individual basis before starting work, while providing collective training for all employees on a regular basis (Information Security Rules Article 14). Recent training sessions were held on July 3, 2018 and September 27, 2018. ・A training program on targeted attack emails is held on a monthly basis to raise awareness. ・To promote IT literacy, all employees are encouraged to pass the IT Passport Examination.
4	Confirming employees' compliance with data management procedures	・The Standards for System Management are set, and tables on authority for tools are maintained based on approvals for applications for account creation/addition/change/deletion. The ledger and registered information are scrutinized on a regular basis (once every three months) (Standards for Information System Management 5 (2)).
V. Technical security control measures		
1	Identifying and authenticating data users	・Email notices are sent to the email addresses registered by customers on log in, legal currency withdrawal, or cryptocurrency remittance (transmission) procedures are taken. This measure, which makes it possible to notify a customer of an unlawful act at an early stage when a third party who pretends to be the customer takes the procedures, has been implemented since June 30, 2018. ・Any account is locked when a wrong password is entered multiple times at the time of log in.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

2	Setting data management classification and access control	・The Cryptocurrency Exchange Service Management System is set up in the security server room at the data center where measures, such as a metal detector, entry/exit management with IC card and biometric authentication, and monitoring cameras, are taken. To enter the building, advance approval by an employee is required. ・The security zone at the head office requires two-step IC Card authentication: when entering general rooms and when entering the security zone. ・Important operations, such as identification procedure, are performed in the security zone, where carrying in smartphone, memo pad and the like is prohibited. Space for storing personal belongings is set up near the entrance. There is an operational rule that allows entry to the security zone only in a way that makes it impossible to take anything out of the zone. ・Entry to and exit from both general rooms and the security zone are monitored using security cameras, and the monitoring records are kept for three months. Whether the security cameras are in operation or not is checked on a regular basis.
3	Controlling data access authority	・Access authority to servers and information is provided only to the minimum necessary persons, and server functions are controlled to be minimum. Computers are set to require users to lock their computer screens or log off when leaving their desks and enter passwords when using computers (Standards for Information System Management 5 (2)).
4	Measures for preventing data leakage, damage, etc.	・Measures at entry points, internal measures, and measures at exit points are being implemented against cyberattacks. Specific measures include two-step authentication at the time of log in; and two-step authentication when a customer transfers funds (fund transfer between accounts, sale and purchase, legal currency withdrawal, cryptocurrency transmission, etc.), which requires entry of the security code for sending notification to a registered email address and the transaction PIN pre-registered by the customer. Note: Two-step setting is a system for safer use of the exchange using a transaction PIN, which is a security code that only the account owner knows, in addition to log in authentication using an ID and password.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

		・Management of the main software in use is performed using a list of server-related software. The latest information about vulnerabilities in the software on the list is obtained. There is a system that, when information about vulnerability is obtained, the system administrator determines the level of required measures in light of the criteria and instructs information system staff to implement measures. (Standards for Information System Management 5 (4)). ・It is ensured that notebook PCs are kept in a cabinet when the users finish their work for the day.
5	Recording and analyzing data access	・Log in/log off accounts, dates, and success/failure, file access success/failure, system log, user/administrator operation log, etc. are acquired with regard to server information systems, including network devices. There is a system that enables information system staff to promptly analyze and report when data exceeds a preset threshold (Standards for Information System Management 5 (3) and other).
6	Recording and analyzing operation of information systems handling data	・All PC operation records are acquired with the use of an integrated log management tool. Device control and access log monitoring are also performed. Use of portable media is not allowed, in principle. When use of portable media is necessary, an application to the department in charge of the operation of the integrated log management must be submitted by following approval procedures, which aims to restrict personal use or use only by a single department.
7	Monitoring and audit of information systems handling data	・Regular inspection of measures, including penetration by white hat hackers, and regular external system audit by an audit firm are performed as part of continual efforts for improvement and review of measures. ・Penetration testing is performed not only as a regular inspection (once a year) but also whenever systems are modified. That has been confirmed with the Report on WEB Application Diagnosis Results and the Report on WEB API Diagnosis Results. It has also been confirmed that, as a result of the diagnoses, improvement efforts have been made for all items by performing re-diagnoses after modifying where needed.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

		・As a measure against unauthorized outside intrusions, an intrusion detection system and an intrusion prevention system have been introduced to perform designated actions, such as notifying the system administrator when an unauthorized action is detected.
VI. Priority security measures		
1	Unique wallet management	・A management system based on unique encryption and other algorithms has been built for hot wallet management, and security is improved with a fine-tuned technical, human, and organizational operations management structure. The mechanism allows implementation of measures that make it difficult for a third party to decrypt a private key even when the hot wallet private key is leaked. In case of contingencies, a certain amount of cryptocurrency is kept in a cold wallet.
2	Multisig	・A mechanism for preventing unauthorized cryptocurrency leakage is in place. Multiple private keys are kept separately so that; even when a private key is stolen, other private keys are stored in safe places.
3	SSL encryption (EV SSL certificate)	・Since inception, BITPoint has used EV SSL（extended validation SSL）certificate at all points accessible for users, so that it is possible to confirm whether the communication partner exists or not more strictly than conventional SSL server certificates.
4	Protection from unauthorized outside intrusions	・The network and hardware is operated and monitored 24 hours a day, every day. In the event of an abnormality, an alert is issued to call attention. Against outside intrusions that may lead to DDoS attacks and consequential service suspension, protection measures, such as reducing and blocking the traffic immediately after detection, are implemented.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

Appendix 1. Rating definitions

【Rating definitions】

AAA_{is}	Extremely high in risk resistance with many excellent elements.
AA_{is}	Very high in risk resistance with excellent elements.
A_{is}	High in risk resistance with partially excellent elements.
BBB_{is}	Sufficient in risk resistance but in the event of significant future environment changes, need to address some elements.
BB_{is}	Not sufficient in risk resistance and in the event of future environment changes, need to address some elements.
B_{is}	Problematic in risk resistance and need to address some elements all the time.
C_{is}	Risk emergence is highly likely

【Supplementary explanation for rating definitions】

AAA_{is}	(Requirement 1) Respond to new threats swiftly and maintain and develop high-level of management all the time. (Requirement 2) Monitor risk all the time and able to respond to situations flexibly.
AA_{is}	(Requirement 1) Have continuous improvement process and maintain and develop high-level of management. (Requirement 2) Incorporate measures against malicious insiders (measures for detection, blocking and prevention).
A_{is}	(Requirement 1) Manage targets in the form of KPIs, using verified process. (Requirement 2) Incorporate measures against malicious outsiders (measures for detection, blocking and prevention).
BBB_{is}	(Requirement 1) Systemically manage and execute procedure manuals, which are clearly defined. (Requirement 2) Incorporate a certain degree of preventive measures (capability to stop incidents in advance).
BB_{is}	(Requirement 1) Unofficial management is observed with dependency on specific personnel. (Requirement 2) Incorporate a certain degree of deterrence (capability to block behaviors) / detection measures.
B_{is}	(Requirement 1) Insufficient management with no established process. (Requirement 2) Insufficient measures for detection (capability to detect occurrence of incidents).
C_{is}	(Requirement 1) Insufficient management with no established process. (Requirement 2) Implement no measures, and constantly under threat.

(Notes) Requirements on lower level of rating needs to be fulfilled when each rating is given. Also, the above Requirement 1 and 2 are supplementary explanation for rating definition and they are subject to changes as needed according to the characteristics at the rated organization and threat changes.

*Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com

Appendix 2. Direction of rating

Direction of rating is the opinion of I.S.Rating on the medium-term direction of the information security rating. To provide a view on the Information Security Rating in a clearer way, we provide all ratings with the direction of rating, in principle.

A rating provided for the first time is a “new rating.” We indicate “positive” when it is highly likely we would review the Information Security Rating for rating upgrade, or “negative” when it is highly likely we would review for rating downgrade, after examination for updating. We indicate “stable” when likelihood of change for the time being is low. We may indicate “direction undecided” in a limited number of cases that do not fall under any of these.

Even the indication of positive or negative for the direction of rating does not predict a change in the Information Security Rating. Even for a department indicated as stable, we may change the Information Security Rating without changing the direction of the rating, depending on the situation.

Appendix 3. Assumed level of rating according to the importance of the information assets owned

Assumed level of rating
according to the importance of the information assets owned

As of October 11, 2018

Legend: Recommended level / Current level

● Assumed business, assumed level, and examples of information assets are provided for reference, and differ according to reasons specific to the company or organization.
● Rating results express I.S.Rating’s opinion on information security measures implemented by the company examined for rating within the rating scope, and do not express a rating of the services or products provided.

Group	Definition of information*1	Assumed level	Assumed business*3	Example of information*1 (Example of core operation of the assumed business)
I	An unlawful event*2 associated with the information may have a serious impact on society as a whole and cause havoc in and outside the country	AAA ------- AA	・Defense-related ・Important infrastructure ・Finance, etc.	・National defense/state secrets ・Crucial information related to human life ・Crucial information related to maintenance and safety of important infrastructure ・Information for disaster response ・Privacy (sensitive) information
II	An unlawful event*2 associated with the information may seriously damage social infrastructure beyond the scope of one organization and cause disruption to part of society	AA ---------- A	・Finance ・Healthcare ・Information/ communication ・Manufacturing ・Commerce ・Services, etc.	・Critical information related to operations of important infrastructure ・Financial/securities information ・Privacy (sensitive)/personal information ・Medical receipt information
III	An unlawful event*2 associated with the information is assumed to cause serious damage to an organization or individual	A ---------- BBB	・Information/ communication ・Manufacturing ・Commerce ・Services, etc.	・Privacy (sensitive)/personal information ・Trade secrets of extreme importance ・An enormous amount of customer lists ・Insider information and financial information before offering
IV	An unlawful event*2 associated with the information is assumed to cause considerable damage to an organization or individual	BBB ---------- BB	・Manufacturing ・Commerce ・Services, etc.	・Important trade secrets (patent before publication, know-how, part of customer list, etc.) ・Personal information within the organization (sensitive information) ・Corporate/personal information of partners
V	An unlawful event*2 associated with the information is assumed to cause limited damage to an organization or individual	BB ---------- B	・Businesses in general	・Information that may not be considered as trade secret (employee’ company phone number, company e-mail address, corporate contact information, etc.) ・Information on normal operations inside the company

*1 For the definition and examples of information, see *Guidance on Outsourcing-Related Information Security Measures*. Table 3. p.16–17 (June 30, 2009, METI)
*2 This table assumes information leakage as an unlawful event in Definition of Information.
*3 Assumed business is estimated by I.S.Rating.

∗Contact details for inquiries I.S.Rating 8F,Kimeta Housing No.20 Bldg., 10-2, Nihonbashihoncho 1-chome, Chuo-ku, Tokyo 103-0023, Japan
TEL:03-3273-8830 http://www.israting.com