

December 25, 2020

To JICPA members

The Japanese Institute of Certified Public Accountants

Remote Work Series No.1

Audit Considerations in Relation to External Confirmation Using Electronic Media or
Processes
- Method using the auditor website -

<<I. Introduction>>

In recent years, there has been an increase in the use of electronic media or electronic processes to confirm the balances of the receivables and payables when auditing financial statements. Also in Japan, auditors have also implemented electronic confirmation systems based on their own websites, and developed methods that use electronic media or processes for confirmation procedures. In particular, we have seen confirmation procedures being performed using electronic confirmation systems not only based on the proprietary websites of individual audit firms, but also electronic confirmation systems based on websites operated jointly by multiple auditors.

In response to this trend, these "Considerations" provide audit considerations in relation to external confirmation using electronic media or processes, which we hope will be of use to the members in their practices.

Furthermore, IT Committee Research Report No. 38 "Audit Considerations in Relation to External Confirmation Using Electronic Media or Processes" (May 18, 2010) (hereinafter "ICRR No.38"), provides a systematic research and exploration of electronic confirmation methods and associated risks, and will be of reference when using these "Considerations".

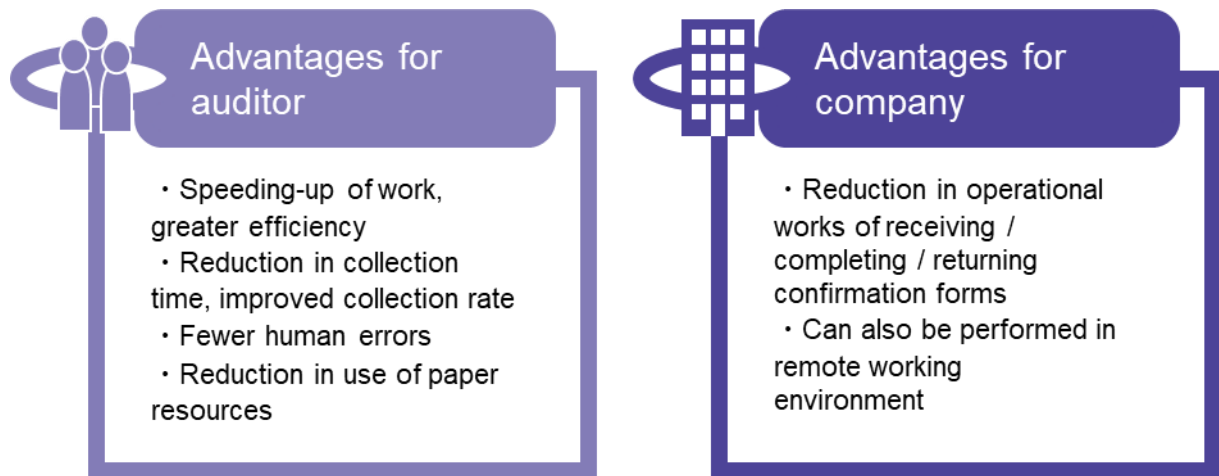
<<II. Electronic confirmation>>

1. What is electronic confirmation?

"Electronic confirmation" in audit procedures performed by auditors refers to the use of electronic confirmation systems implemented and operated by auditors or audit clients or third parties, in which requests for confirmation are sent, or responses to such requests are obtained, via electronic media or electronic processes.

ICRR No.38 discusses various methods to perform electronic confirmation, such as the use of paper documents to implement an external confirmation request, with the responses obtained either in electronic format or using electronic processes. The advantages of the use

of electronic confirmation for both auditors and companies are as shown in the following diagram.



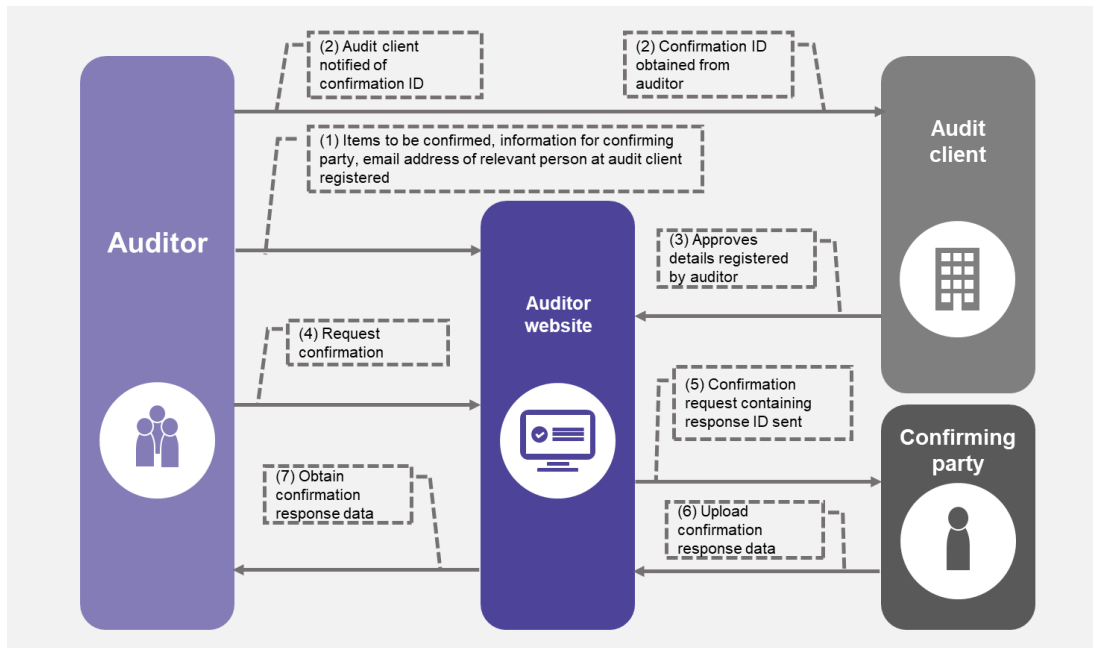
Electronic confirmation has the benefits described above, especially during the novel coronavirus infectious disease (COVID-19) pandemic, where remote work has become required to prevent the spread of infection. The approach has been recently appropriate not only to obtain electronic responses, but also performing information requests via electronic media or electronic processes. Also, in recent years in Japan, we have seen auditors developing and using electronic confirmation systems, either independently or jointly with others.

2. Electronic confirmations covered by these “Considerations”

In these “Considerations”, we cover methods in which auditors performing an audit procedure requests and obtains external confirmation response using electronic confirmation systems based on websites implemented and operated by auditors.. External external confirmation using an auditor website includes the use of electronic confirmation systems based on websites operated jointly by multiple auditors.

3. What is external confirmation using an auditor website?

“Confirmation using an auditor website” refers to a system hosted on a website built or operated by an auditor that enables a confirming party to upload confirmation response data to a specific URL, and the auditor to access this specific URL to obtain the confirmation response data. An example of an external confirmation using an auditor website is in the diagram below.



- (1) The auditor accesses the designated website and registers the items to be confirmed, the information for the confirming party, and the email address of the relevant person in charge at the audit client (alternatively the audit client may perform the registration).
- (2) The auditor notifies the relevant person at the audit client of the confirmation ID generated at the time of registration.
- (3) The relevant person at the audit client accesses the website, enters the confirmation ID received from the auditor, and approves the details registered by the auditor.
- (4) The auditor accesses the website and requests the confirming party for confirmation of the items approved by the relevant person at the audit client.
- (5) The website sends a confirmation request containing a response ID to the confirming party, either in paper form or in electronic form via an electronic process. In cases where the confirmation request from the auditor is made not in paper form, there may be measures in place to communicate, via an electronic process, the fact that the audit client has agreed to the auditor performing the confirmation procedure, to the confirming party (ICRR No.38, II 7.(1)(i), (ii)).
- (6) The confirming party uploads the confirmation response data associated with the registered audit client to the website.
- (7) The auditor accesses the website and obtains the confirmation response data in the form of an electronic file.

4. Comparison with the “third-party website” method cited in ICRR No.38

ICRR No.38 discusses a method that uses a “third-party website”. This “third-party

website” method involves a system within a website hosted by a third-party service provider designated by the confirming party, in which the confirming party uploads the confirmation response data to a specific URL. We have also seen examples, mostly overseas, of financial institutions outsourcing the process of confirmation responses to third-party service providers. There are many similarities between the method using the auditor website and the method using the third-party website cited in ICRR No.38, but they may differ on the following points.

- (1) In the case of the method using the third-party website, the auditor generally sends a confirmation request to a confirming party registered on the website. In the case of the method using the auditor website, the auditor may need to individually register details of confirming parties before performing each confirmation request. For both methods using the auditor website and the third-party website, there is a certain level of risk that someone other than the registered confirming party makes a response. In the case of the third-party website, the third party service provider and the confirming party agree to the continuous use of a fixed URL. Whereas, in the method using an auditor website, the confirming party is not fixed and differs for each confirmation request, the auditor need to obtain the email address and other information of the confirming party from the audit client on each occasion. For that reason, risks associated with electronic confirmations, such as denial of responded confirmation request or the impersonation of a confirming party (refer to ICRR No.38 II 3), may be relatively high using an auditor website compare with third party’s website.
- (2) The method using a third-party website consists of a system within a website hosted by a third-party service provider, but in the method using an auditor website, the electronic confirmation system is implemented and operated on the auditor’s website. For that reason, it is often the case that the auditor’s electronic confirmation system is easier to understand, and the reliability of the information is easier to verify, than in the case of the method using a third-party website.

	Method using third-party website	Method using auditor website
Operator of website	Third party	Auditor
Use of website	Designated by confirming party	Designated by auditor
Confirmation request method	Auditor sends confirmation request to confirming party who has already been registered on the website	Information related to the confirming party obtained from audit client and entered individually for each confirmation before performing request
Risks associated with electronic confirmation such as impersonation or denial after replying confirmation request	Relatively low	Relatively high
Understanding electronic confirmation system and verification of the reliability of information	Relatively difficult	Relatively easy

<<III. Considerations>>

1. External confirmation using electronic methods based on ASCS 505

Paragraph 10 of Auditing Standards Committee Statement 505, “External Confirmations” (hereinafter, “ASCS 505”), states that “if the auditor identifies factors that give rise to doubts about the reliability of the response to a confirmation request, the auditor shall obtain further audit evidence to resolve those doubts.” Furthermore, Paragraph A11 states that “All responses carry some risk of interception, alteration or fraud. Such risk exists regardless of whether a response is obtained in paper form, or by electronic or other medium.”

Risks associated with responses to confirmation procedures, such as reliability, falsification and fraud, exist irrespective of whether the confirmation procedure is performed in paper form using mail, or by electronic methods. However, it needs to be kept in mind that the nature and the assessment of these risks varies depending on whether the external confirmation is performed using electronic methods or using paper, and consideration is necessary to evaluate whether these risks have been reduced to an acceptable low level.

2. Risks associated with external confirmation using an auditor website

Risks associated with external confirmation using an auditor website basically consist of risks such as impersonation of the confirming party and denial after replying confirmation, as described in ICRR No.38, and are composed of the following four risks.

- (1) Risk that the response is not obtained from appropriate source of information
- (2) Risk that the confirming party does not have the authority to respond
- (3) Risk that the integrity of the information transmission has been compromised
- (4) Risk that the confirming party denies the details of the response

Of these, “(4) Risk that the confirming party denies details of the response” refers to the risk that, in the event that the confirming party subsequently denies their involvement or the details of the response, the auditor cannot present any evidences to disprove them. Moreover, it needs to be kept in mind that the details and assessment of such risks will vary depending on the nature of the electronic confirmation system based on the auditor website.

3. Example of responses to the risks associated with external confirmation using an auditor website

Methods assumed to mitigate the above-mentioned risks associated with confirmation using an auditor website may include those listed below.

The following include some methods that may not mitigate risks sufficiently when used independently. Depending on the situation, careful assessment may be required to ascertain whether it is necessary to use a number of different methods in combination, or to consider that it may not be possible to obtain an appropriate response when the confirming party is a individual person. In addition, depending on the level of inherent risks, audit risk may not be able to be reduced to an acceptable low level even when combinations of these methods are used. For that reason, it needs to be kept in mind that careful assessment may be required, depending on the situation.

The responses performed more efficiently at the audit firm level are included rather than at the level of individual audit teams.

It also needs to be kept in mind that in examples 1, 5, 6 and others, it is important to obtain the cooperation of the audit client and the confirming party.

	Possible Responses	Risks associated with confirmation using an auditor website (referto 2.)			
		(1) Risk that the response is not obtained from appropriate source of information	(2) Risk that the confirming party does not have the authority to respond	(3) Risk that the integrity of the information transmission has been compromised	(4) Risk that the confirming party repudiates the details of the response
(Example 1)	Involvement of multiple persons in the confirmation response	⊗	⊗		
(Example 2)	Using the telephone to confirm with the confirming party	⊗	⊗		
(Example 3)	Additional procedures related to the confirming party	⊗	⊗		
(Example 4)	Investigating the appropriateness of the domain	⊗	⊗		
(Example 5)	Using electronic signatures	⊗	⊗		⊗
(Example 6)	Using the Ministry of Justice's electronic certification system based on commercial registration	⊗	⊗		
(Example 7)	Use of fraud detection functions in relation to IP addresses	⊗	⊗		
(Example 8)	Confirming the reliability of the auditor website			⊗	
(Example 9)	Obtaining pledges, etc. from confirming parties		⊗		⊗

*The ⊗ symbol denotes the main risks that may need to be managed in each example of the response.

(Example 1) Involvement of multiple persons in the confirmation response

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, it may be effective to use multiple respondents, and to specify the route for the confirmation response so that it goes via the superior of the confirming party, or via the person responsible for accounting.

In addition, after the auditor has obtained a response to the confirmation request, sending a report by email or some other method not only to the confirming party but also to their superior, reporting that confirmation has been obtained from that person, and thus communicating to their superior and others that a confirmation response was performed by that person, may be an effective way of managing such risks.

The involvement of multiple persons in the response to a confirmation request may be an important factor in restricting the confirming party to an appropriate response.

When requesting the involvement of a superior in a matter involving the response to a confirmation request, it is proper for the auditor to have an understanding of that person's responsibilities and their position relative to the duties performed by the confirming party, and to assess whether their involvement is appropriate. When a response has been obtained, it is important to confirm that the response has come only via the specified superior.

(Example 2) Using the telephone to confirm with the confirming party

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, when sending a confirmation request, the auditor is expected to check that the confirming party actually exists, and that they have the appropriate authority to respond, determining whether requests are properly addressed by, for example, telephoning the confirming party to test the validity of some or all the addresses before sending out the confirmation requests (Paragraph A6, ASCS 505).

In cases where the email address of the confirming party is a group email address, there may not be one individual specified as the confirming party. Because this suggests a higher risk that the response is not obtained from an appropriate source of information, or that the confirming party does not have the authority to respond, in addition to identifying the confirming party using the group email address, the auditor needs to consider whether they have appropriate authority within the organization to respond to confirmation requests. However, similarly to the way a company that is a confirming party may formally notify the audit client of a dedicated address for responding to electronic confirmation requests, it may be more reliable to use a group address for registering a confirming party rather than the address of an individual.

In addition, when the confirming party replies by email, the auditor may in some cases telephone the confirming party to verify that it was actually them who sent the response (Paragraph A14, ASCS 505).

In cases where a confirming party whose identity was checked by telephone in previous years is being asked for another confirmation response, or in cases where, for example, the administrator of the auditor website consults the financial institution in advance in relation to the attributes of the confirming party, their method of response, and their email address, and the auditor determines that the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond has been reduced to an acceptable low level, it may be possible to omit telephone confirmations, investigations into the appropriateness of the domain (discussed below) and comparisons using fraud detection procedures in relation to IP addresses.

(Example 3) Additional procedures related to the confirming party

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, the auditor may take actions such as the following to confirm that the confirming party exists, and that they are an appropriate confirming party.

- Inspecting the history of communication between the relevant person in charge at the audit client and the confirming party (including inspecting the business card of the confirming party obtained by the audit client)
- Investigating whether the name of the confirming party is included in documents, etc. obtained by the audit client from the confirming party in relation to transactions, etc.

Also, in the event that doubts arise about the reliability of the information after confirmation has been obtained, in cases where a confirmation response of only the account balance has been obtained, the auditor may consider, for example, sending via the auditor website or some other route a request for additional responses, such as documents providing a breakdown to support the details of the initial response.

(Example 4) Investigating the appropriateness of the domain

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, the appropriateness of the domain in the confirming party's email address may be investigated.

In terms of investigating the appropriateness of the domain, in cases where an email address for inquiries is available in the confirming party's official website, the auditor may check for consistency of the domain of the email address.

An alternative method would be to verify the registration status of the domain used in the confirming party's email address,

For checking the registration status of an email address domain, the so-called Whois (<https://whois.jp/rs.jp/>) search service can be used to confirm whether an email address has been recorded in the registry, as well as the organization name, and information related to the domain administrator. In particular, "co.jp" domains cannot be obtained without having some form of corporate status in Japan, and only one such domain can be obtained by each individual company or organization, with the presentation of company registration information being required at domain registration, so registered corporations should actually exist, and users of the domain are likely to belong to the corporation.

For that reason, it may be informative to check whether the confirming party's email address domain is appropriate, using the actual email address used to provide the response.

Be aware that for domains other than “co.jp” domains, it is not necessarily the case that the registry confirms the actual existence of the organization before registering a domain name.

In some cases, as a result of a domain search, it is found that the domain is registered by the registry, but it seems likely that the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond has not been reduced to an acceptable low level. In such circumstances the auditor may consider making inquiries by means of a telephone call to the confirming party, or sending an email to the domain administrator, in addition to the domain search.

(Example 5) Using electronic signatures

In order to manage the risk that the response is not obtained from an appropriate source of information, the risk that the confirming party does not have the authority to respond, or the risk that the confirming party will deny the details of the response, the auditor may request the confirming party to add an electronic signature to the response, so as to prove that the organization to which the confirming party belong actually exists.

By “electronic signature” we mean an encryption device, as prescribed in Act on Electronic Signatures and Certificate Business, used for the purpose of proving the creator of electrical information, and that if someone made edit, users of the electrical data can figure out changes made to the electrical data. It is assumed that an electronic certificate is issued by a certification business operator to confirm that the electronic signature has been added by the person to whom it belongs. In cases where such an electronic signature is put on the response from a confirming party via an electronic process, the auditor can confirm that the response from the confirming party was truly replied by the confirmer, and that the electrically signed document has not been falsified, which is a beneficial outcome.

For witness-type electronic signatures, the email address of the creator of the information may be included in the properties of the electronic signature or in the agreement concluded between the creator and the electrical signature service provider.

In such cases, it is possible to check whether the response was obtained from the appropriate source of information expected at the time the request was made by comparing this email address to the email address of the confirming party used in a confirmation request performed via an electronic process.

(Example 6) Using the Ministry of Justice’s electronic certification system based on commercial registration

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, the auditor may request the confirming party to attach the electronic certificate issued by the registry for the company or corporation (http://www.moj.go.jp/MINJI/minji06_00028.html) to the response, so as to prove that the organization to which the responding party is affiliated actually exists.

Unlike the electronic signature system, which aims to confirm the identity of the creator of information, this certification system is a method for proving that commercial registration has been conducted using an electronic medium instead of a paper-based seal-registration certificate, and in theory it could be applied to electronic transactions between companies. However, its use is limited to online applications and notifications for governmental and local governmental agencies, and there has not been much development for use in transactions between companies. In addition, it needs to be kept in mind that certain measures must be taken beforehand, when used for an application the user (confirming party) must perform the initial procedure at the registry, and the auditor must install special software to read the electronic certificate.

(Example 7) Using fraud detection procedures in relation to IP addresses

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, an electronic confirmation system using an auditor website can compare the IP address of the responding user and the IP address of the audit client to check whether they are the same. In other words, checks can be made as to whether the confirming party and the audit client are the same.

Using electronic technology in this approach allows the auditor to comprehensively detect situations in which the confirming party may be the same as the audit client. In addition, the audit client can be discouraged from impersonating the confirming party.

Nevertheless, in order to implement this approach, the auditor may obtain the IP address of the audit client in advance, and may perform procedures to compare this to the IP address of the confirming party's electronic system. Furthermore, in cases where someone, impersonating the confirming party, accesses the auditor website outside the audit client network (for example, using an individual email address), the above-mentioned detection procedure will be ineffective, and so provides only limited defense against impersonation. Therefore, it may be used in combination with an investigation of the appropriateness of the domain.

(Example 8) Confirming the reliability of the auditor website

It is not easy to detect changes to a confirmation response performed electronically, and there is a risk that fraudulent behavior such as inappropriate manipulation or falsification at the time of sending or receiving may go undetected, compromising the integrity of the information transmission. Whether or not this risk can be mitigated to the required level depends on the auditor website system, and so the auditor needs to take measures that are appropriate to the circumstances. For example, the administrator is expected to assess continuously whether the design of the internal controls built into the auditor website is suitable for the circumstances, or take steps to rectify the situation in cases where there is a deviation from predetermined processing. In addition, in cases where the auditor website is used jointly by multiple auditors, they may decide to use service auditor's report from an independent third party in relation to internal controls for outsourced operations.

(Example 9) Obtaining pledges, etc. from confirming parties

It is not easy to determine whether a confirming party has the proper authority to provide a response, and there is a risk that if the confirming party subsequently denies the details of the response, the auditor cannot present any evidences to disprove them. In order to mitigate such risks by a certain level, procedures could be incorporated to enable confirmation responses on the auditor website to include statements to the effect that the confirming party has the necessary authority in the confirming organization, that the response is accurate, and that the response takes precedence over other responses based in paper form.