



DPC: 24/30466020 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 04 September 2024

Origin: International

Latest date for receipt of comments: 28 October 2024

Project No. 2022/02688

Responsible committee: IST/12 Financial services

Interested committees:

Title: Draft BS ISO 18960 Security controls and implementation guidance for third party payment service providers.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 28 October 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 18960

Security controls and implementation guidance for third party payment service providers

ICS: 35.240.40

ISO/TC 68/SC 2

Secretariat: BSI

Voting begins on:
2024-09-04

Voting terminates on:
2024-11-27

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/DIS 18960:2024(en)

© ISO 2024



Documents

Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Security governance controls	2
5.1 Service security policies	2
5.1.1 Establishment of information security policy	2
5.1.2 PII protection policy	3
5.1.3 User permission	3
5.1.4 User complaint handling policy	4
5.2 Roles and responsibilities	4
5.2.1 TPPSP security management organization	4
5.2.2 Guide for users about security considerations	4
5.3 Risk management	5
5.3.1 Establishing risk management process	5
5.3.2 Performing risk assessment and treatment	5
5.4 Documentation	5
5.4.1 Documented information	5
5.4.2 Management of documented information	6
5.5 Monitoring, review and improvement	6
5.5.1 Preservation of logs on incident responses and monitoring	6
5.5.2 Regular security review	6
5.5.3 Continual improvement	6
6 Cross-functional controls	7
6.1 Asset management	7
6.2 Access management	7
6.2.1 Access management of administrators	7
6.2.2 Access management of administrator programs	8
6.2.3 Designation and access management of terminals	8
6.3 Supplier security	9
6.3.1 Selection and management of suppliers	9
6.3.2 Identification and management of the use of cloud services	9
6.4 Data security	10
6.5 TPP service continuity	10
7 Function specific controls	11
7.1 Vulnerability management	11
7.1.1 Preparation of incident response procedures	11
7.1.2 Education and training for incident response	11
7.2 Human security	12
7.2.1 Establishment and implementation of information security education plans	12
7.2.2 Completion of information security education	12
7.2.3 Confidentiality and non-disclosure agreement	12
7.2.4 Segregation of duties	13
7.2.5 Removal or adjustment of access rights at termination and change of employment	13
7.3 Physical security	14
7.3.1 Designation of secure area and entry control	14
7.3.2 Management of secure area's check-in and check-out	14
7.3.3 Management of working environment security	15
7.4 Server security	15

ISO/DIS 18960:2024(en)

7.4.1	Prevention of malware infection and information leakage	15
7.4.2	Removal of unnecessary functions	16
7.4.3	Important service operation on dedicated server	17
7.4.4	Public web server security	17
7.4.5	Security patch management	17
7.5	Network security	18
7.5.1	Control on remote management through Internet	18
7.5.2	DMZ configuration	19
7.5.3	Use of private IP and network segregation	19
7.5.4	Wireless network security	20
7.5.5	Application of secure communication when communicating with external organizations	20
7.6	TPP application security	20
7.6.1	Identification of security requirements during design stage	20
7.6.2	Web application security	21
7.6.3	Mobile application security	23
Annex A (informative) Relation between ISO 18960 and ISO 23195		25
Bibliography		27

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee [or Project Committee] ISO/TC [or ISO/PC] ###, [name of committee], Subcommittee SC ##, [name of subcommittee].

This second/third/... edition cancels and replaces the first/second/... edition (ISO #####:#####), which has been technically revised.

The main changes are as follows:

— xxx xxxxxxxx xxx xxxx

A list of all parts in the ISO ##### series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Fintech-centric financial innovation is indeed happening worldwide, and the proliferation of third-party payment service providers (TPPSPs) is a significant aspect of this trend. TPPSPs offer innovative and convenient payment solutions, transforming traditional payment methods and reshaping the financial landscape. Furthermore, through TPP service, the TPP has facilitated the provision of various financial services across borders between member countries reducing barriers to entry.

Since most of the information used by TPPSP includes the customer's personally identifiable information (PII), the security issue of the TPPSP becomes even more important. In addition, small and medium-sized TPPSPs may face greater risks due to their limited capacity for system implementation. Thus, payment service providers that provide TPP services with customer information have a responsibility to review the security measures and practices of the TPPSPs.

In accordance with the characteristic requirements, each TPPSP should establish and operate specific security controls on its own.

While ISO 23195 covers security objectives for TPPSP systems, this document covers organization-wide security controls for TPPSP which operates the systems based on the relevant control measures such as policies, human resources, physical environment, application development, system operation, audit, and continual improvement, etc. The security controls for TPPSP covered in this document help to achieve the security objectives in ISO 23195.

On the other hand, ISO/IEC 27002 is designed for organizations of all types and sizes as a reference for determining and implementing controls for an information security management system (ISMS) based on ISO/IEC 27001. This document covers consolidated controls which are specific for TPPSP reflecting business characteristics of financial service including privacy issues.

This document introduces security controls for TPPSP. The controls for TPPSP are categorized into governance security controls, cross-functional controls, and function-specific controls.

Firstly, governance controls deal with overarching policies that guide an organization's approach to security. Specific elements of these controls are service security policies, roles and responsibilities, risk management, documentation, monitoring, review, and improvement.

Secondly, this document introduces cross-functional controls that are necessary throughout the organization. This includes asset management, access management, supplier security, data security, and TPP service continuity.

Lastly, function-specific controls that are tailored to specific areas of an organization's operations are explained. This includes vulnerability management, human security, physical security and system security such as server, network and application security.

Additionally, [annex A](#) provides a mapping table which shows how the controls outlined in this document align with the security objectives provided in ISO 23195.

Security controls and implementation guidance for third party payment service providers

1 Scope

This document gives guidance on security controls and implementation guides for the third-party payment service providers (TPPSPs). This document deals with the overall security controls of TPPSPs from developing and testing to installing, operating, and auditing the system. These security controls consist of

- Security governance controls
- Cross-functional controls
- Function-specific controls

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 23195:2021, *Security objectives of information systems of third-party payment services*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 governing body

person or group of people who are accountable for the performance and conformance of the TPPSP

3.2 sensitive information

information that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual, organization, national security or public safety

Note 1 to entry: While “important information” refers to comprehensive information that requires security, “sensitive information” refers to information that can cause damage if exposed and emphasizes the importance of confidentiality.

[SOURCE: ISO/IEC 27002:2022, 3.1.33]

3.3 topic-specific policy

intention and direction on a specific subject or topic, as formally expressed by the appropriate level of management

[SOURCE: ISO/IEC 27002:2022, 3.1.35]

3.4**personally identifiable information**

information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person

[SOURCE: ISO/IEC 29100:2024, 3.7]

4 Abbreviated terms

PMS	patch management system
GB	governing body
PII	personally identifiable information
ACL	access control list
NAT	network address translation
WIPS	wireless intrusion prevention system
VPN	virtual private network
CSRF	cross-site request forgery
RFP	request for proposal

5 Security governance controls**5.1 Service security policies****5.1.1 Establishment of information security policy**

TPPSPs should implement and regularly review a formal documented security policy for the financial services they operate. Information security policies shall be established, documented, announced and be only implemented after the TPPSP GB approval and prior to offering the financial service to the market. Top-level information security policies shall be established and approved by the top management so they can serve as the basis of all information security activities conducted by the organization.

These policies shall include the following but not be limited to:

- The intention and direction of the top management for information security policy;
- Purpose, scope, and responsibilities of the organization's information security, including the information security risk management function;
- The grounds for information security activities performed by the organization.

TPPSP shall manage the list of relevant laws and regulations that affect the organization and the financial services operated. Also, TPPSP should consider the references of the appropriate technical standards used by the organization to implement the security policy.

The documents on information security policies and topic-specific policies should be disclosed through educational sessions, e-mails, notice boards, etc. to appropriate employees, allowing them to view the documents at any given time.

EXAMPLE Materials subject to inspection:

- Documents on information security policies and topic-specific policies;

- Materials confirming the announcement status of the documents on information security policies and topic-specific policies.

5.1.2 PII protection policy

The TPPSP should assess the specific risks for the customer PII data prior to offering their services to the market. Based on this risk assessment, the TPPSP should establish a documented specific PII security policy. This policy should include the measures and procedures to effectively manage the risks identified for the authenticity, integrity and confidentiality of PII data. This policy should also include safeguards protecting against intrusions and PII misuse and should include provisions to ensure that these risks are properly monitored during the operation of the services.

This security policy should be sufficiently transparent for the customer, easily read and understood, enabling to make an informed consent on the processing of their PII. TPPSPs should be open with customers about the sources used to collect PII data (e.g. merchants), what PII data are collected, why they are collected and how they are processed.

PII protection policies shall be opened to the public to increase user awareness, and consents to PII processing shall be received from users according to applicable laws and regulations. When a service has membership or collects PII, a PII protection policy shall be established and disclosed at a site that users can easily access, for example web page or homepage of the service.

Requirements stipulated by applicable laws and regulations should be included, for example, PII to be collected, purpose of use and collection methods, periods of retention and utilization, right to refuse and disadvantages of refusal.

Required and optional information should be classified appropriately so that a minimum amount of PII is collected and consented to achieve the purpose of the service.

EXAMPLE Materials subject to inspection:

- A web page showing PII protection policy and full text of the policy;
- A web page displaying the agreement on collection and use of PII of users.

5.1.3 User permission

When using PII for accessing to account information and requesting financial transaction, the customer should be notified in advance by the TPPSP.

When the financial institution needs access to the user's PII and credit information and to make electronic financial transaction orders, it should provide sufficient information to the user and obtain his/her permission.

EXAMPLE The information to be notified:

- Purpose of access to the user's information and electronic financial transaction order;
- List and types of financial electronic transaction orders and user PII that can be accessed by the institution;
- Valid period of the permission and its withdrawal method.

The duration of access to customer PII should be appropriately defined to mitigate the risk of data misuse. The TPPSP should only access the PII data needed for providing the service and not use any PII data for other purposes than those for which user permission has been granted by the customer.

The organization shall provide with effective means to enable the customer to verify that the data withdrawn by the TPPSP correspond effectively to the information requested for which his/her consent was granted.

EXAMPLE Provision of information:

- Viewing functions on websites, posting available contact for information request.