



BSI Standards Publication

Security controls and implementation for third party payment service providers — Guidance and requirements

National foreword

This British Standard is the UK implementation of ISO 18960:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 24988 0

ICS 35.240.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



**International
Standard**

ISO 18960

**Security controls and
implementation for third party
payment service providers —
Guidance and requirements**

*Contrôles de sécurité et mise en œuvre pour les prestataires de
services de paiement tiers — Recommandations et exigences*

**First edition
2025-08**

Reference number
ISO 18960:2025(en)

Full document details: BS ISO 18960:2025

© ISO 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

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	3
5.1 Service security policies	3
5.1.1 Establishment of information security policy	3
5.1.2 PII protection policy	3
5.1.3 User permission	4
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	5
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	6
5.4.1 Documented information	6
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	7
5.5.3 Continual improvement	7
6 Cross-functional controls	7
6.1 Asset management	7
6.2 Access management	8
6.2.1 Access management of administrators	8
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
7.1.3 Documentation of vulnerability management policy	12
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	13
7.3.1 Designation of secure area and entry control	13
7.3.2 Management of check-in and check-out of secure area	14
7.3.3 Management of working environment security	14

ISO 18960:2025(en)

7.4	Server security	15
7.4.1	Prevention of malware infection and information leakage	15
7.4.2	Removal of unnecessary functions	15
7.4.3	Important service operation on dedicated server	16
7.4.4	Public web server security	16
7.4.5	Security patch management	16
7.4.6	Data sanitization	17
7.5	Network security	17
7.5.1	Control on remote management through Internet	17
7.5.2	Demilitarized zone configuration	17
7.5.3	Use of private IP and network segregation	17
7.5.4	Wireless network security	18
7.5.5	Application of secure communication when communicating with external organizations	18
7.6	TPP application security	19
7.6.1	Identification of security requirements during design stage	19
7.6.2	Web application security	19
7.6.3	Mobile application security	21
Annex A (informative) Relation between ISO 18960 and ISO 23195		22
Bibliography		24

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

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 (TPP) 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 and thus reduced 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 can 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 operate the systems based on the relevant control measures. The control measures include policies, human resources, the physical environment, application development, system operation, audit and continual improvement. 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 based on ISO/IEC 27001. This document covers consolidated controls that are specific for TPPSP and that reflect the 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 for third party payment service providers — Guidance and requirements

1 Scope

This document gives requirements and guidance on security controls and implementation for 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 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 third-party payment service providers

Note 1 to entry: Governing body can include external regulatory representatives.

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, modified — Note 1 to entry has been added.]

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, modified — The Notes to entry have been removed.]

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, modified — The Notes to entry have been removed.]

4 Abbreviated terms

ACL	access control list
CEO	chief executive officer
CISO	chief information security officer
DB	database
DBMS	database management system
DMZ	demilitarized zone
FTP	file transfer protocol
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure
IDC	internet data center
IDS	intrusion detection system
IP	internet protocol
IPS	intrusion prevention system
MAC	message authentication code
OS	operating system
PC	personal computer
PII	personally identifiable information
PMS	patch management system
RTO	recovery time objective
SFTP	secure shell file transfer protocol
SSID	service set identifier
TLS	transport layer security
TPP	third party payment

TPPSP	third party payment service provider
URL	uniform resource locator
USB	universal serial bus
VPN	virtual private network
WAP	wireless access point

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 and announced. These policies should only be implemented after the governing body of the TPPSP has granted 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 TPPSP.

These policies shall include at least the following:

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

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

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

NOTE For general requirements of information security policy, see ISO/IEC 27001.

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 and easy to read and understand, so the customer can give 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 open to the public to increase user awareness. PII shall only be processed for users who have given consent. 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, e.g. the web page or homepage of the service.