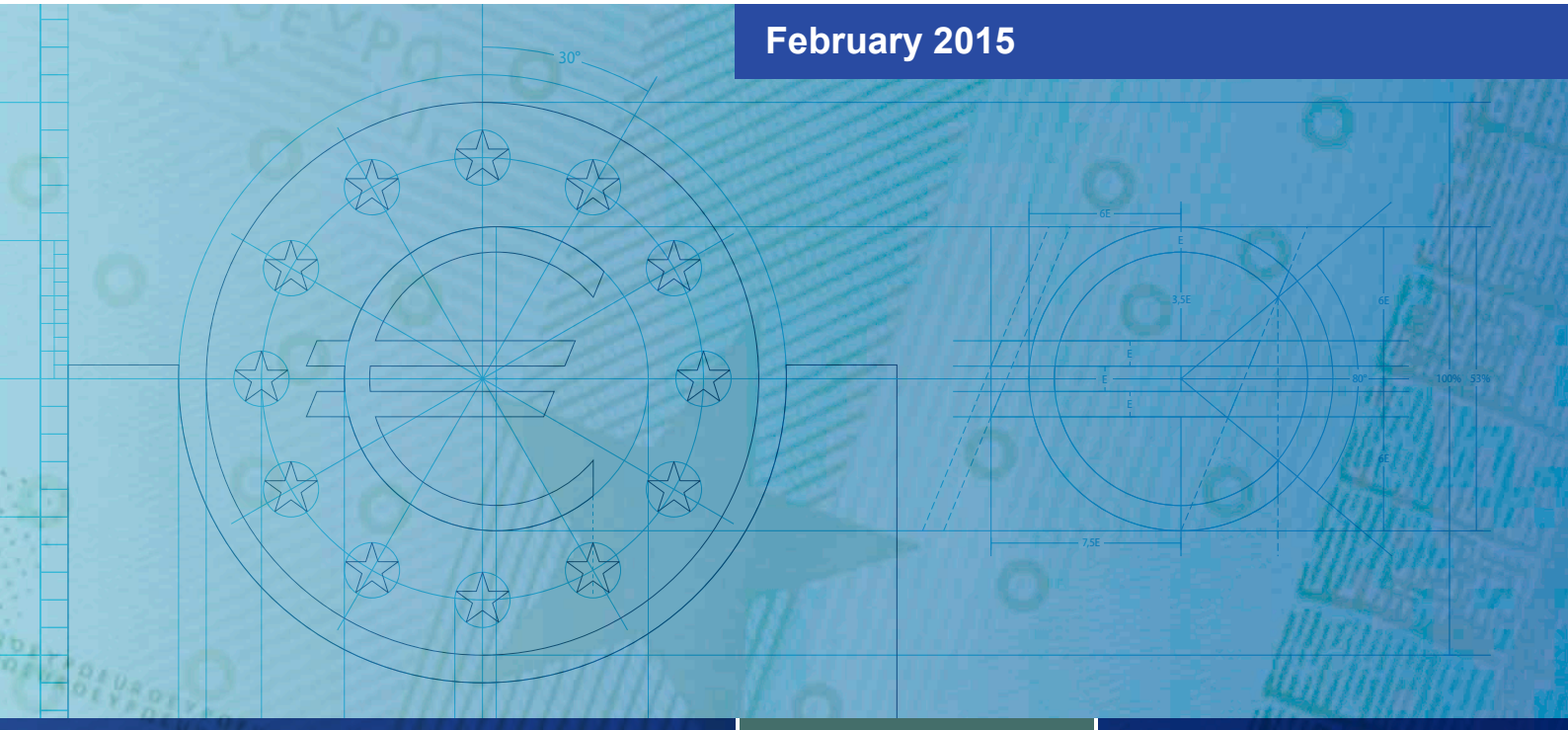
EUROPEAN CENTRAL BANK

EUROSYSTEM

Guide for the assessment of card payment schemes against the oversight standards

February 2015



Postal address
60640 Frankfurt am Main
Germany

Telephone
+49 69 1344 0

Website
www.ecb.europa.eu

ISBN 978-92-899-1510-6 (online)
EU catalogue number QB-01-15-070-EN-N (online)
Digital object identifier: 10.2866/11261

CONTENTS

INTRODUCTION

The Eurosystem has developed oversight standards for card payment schemes (CPSs), with a particular focus on the security and efficiency of card payments. The "Oversight framework for card payment schemes – standards" was published in January 2008. This assessment guide supports a comprehensive and efficient assessment against these standards.

This assessment guide is intended both for the CPSs' governance authorities (GAs) responsible for ensuring compliance, and for the overseers conducting the oversight of both national and international CPSs based on the Eurosystem oversight standards for CPSs. It has been updated with the incorporation of the "Recommendations for the security of internet payments" that were approved by the Governing Council in January 2013, as well as the "Assessment guide for the security of internet payments" of February 2014. Certain requirements coming from these two documents may be directly addressed to payment service providers (PSPs). As explained in the "Harmonised oversight approach and oversight standards for payment instruments", the Eurosystem intends to avoid overlaps and duplication of work between the oversight standards for payment instruments and other oversight activities or activities carried out by supervisory bodies. Accordingly, overseers may consider relevant assessments or activities of supervisory bodies when conducting their assessment of those specific requirements.

The assessment guide outlines the general requirements that overseen CPSs should follow in order to provide the general business and statistical information needed, and to respond properly to all assessment questions (AQs), following the specific oversight guidelines on what should be expected by the overseers for each AQ. In principle, the CPSs are expected to answer each of the AQs with a "Y" or "N", providing sufficient justification and evidence, and attaching supporting background information and documents. This assessment guide enables the overseers of national and international schemes to be transparent towards the market concerning the oversight assessment process and should also help to avoid disagreements and misinterpretations across countries. As a result, this assessment guide provides the overseer with reasonable assurance that the AQs were answered appropriately. Finally, it should be used as a guide for determining the CPSs' level of observance for each of the oversight standards and will serve as the broad layout for the final oversight report.

The Eurosystem addresses its oversight standards to the governance authority of the CPS. The concept of **"governance authority"** with regard to CPSs relates more to specific functions than to an individual entity. It is possible that the functions are assumed by different entities at different levels. Each entity is responsible for the function(s) it performs within the scheme and is the addressee of the oversight standards in this respect. If there is more than one entity for a given scheme, they are jointly accountable for the overall functioning of the CPS, for promoting the payment instrument, for ensuring compliance with the scheme's rules and for setting clearly defined, transparent, complete and documented boundaries for their responsibilities within this scheme. These entities must then jointly ensure that all relevant standards of the oversight framework are met. Oversight activities will be conducted taking into account the division of responsibilities. The assessment guide uses the wording "the GA requires service providers and/or PSPs to" when a topic is addressing the general functioning of a payment instrument and has the potential to significantly impact a scheme. Nevertheless, all measures taken and all activities carried out within the scheme should be in line with the security policies defined by the actor(s) performing governance functions. The Eurosystem focuses its approach to the oversight of payment instruments on issues of scheme-wide importance that are under the control of the governance authority of the scheme providing the payment instrument.

Section 1 outlines the reporting methodology to be applied, the general information to be provided by each CPS, the statistical information to be reported and the requirements for incident reporting.

Section 2 lists the assessment questions, which focus exclusively on gathering specific information that the Eurosystem considers indispensable for a reliable assessment of a CPS. Although the AQs are very detailed, they should not be considered prescriptive as regards the organisation of the card payment business. Indeed, the Eurosystem is aware that different options could be equally satisfactory in terms of reaching an acceptable level of resilience for each CPS oversight standard. This will be taken into account throughout the assessment process. The assessment questions are complemented by a check-list providing further guidance on how to ensure that a question is answered in sufficient detail and interpreted in a consistent way. The items in these check-lists describe generic situations which may not be of relevance for a specific scheme. It must be noted that a limited number of these items refer to best practices outlined in the "Recommendations for the security of internet payments". Compliance with such check-list items is not mandatory and will not be scored during the assessment process. The GA is nevertheless encouraged to indicate its compliance with them.

I REPORTING METHODOLOGY AND INFORMATION REQUIRED FROM CARD PAYMENT SCHEMES

1 REPORTING METHODOLOGY

1.1 INVENTORY OF DOCUMENTS AND INFORMATION

The GA should attach a detailed inventory describing all documents and information provided.

All information should be submitted in electronic form whenever possible. The enclosed documents and information[1] should preferably be in English. Upon the request of the overseer, a translation of the original or a copy of such a translation verified by the GA should be provided.

1.2 REFERENCES

Where possible, the GA may submit only references to documentation and information that has already been submitted to the overseeing authority.

The overseeing authority may require additional documents to be submitted with the purpose of ascertaining all the facts and circumstances required for the assessment of the card payment scheme (CPS) against the applicable oversight standards.

1.3 ASSESSMENT QUESTIONS

With regard to the assessment questions presented in Section 2 of this guide, the GA is required to:

- answer all assessment questions with all information and explanations needed by the overseer for a reasonable assurance and provide appropriate reasoning and background documentation;
- provide information about any changes that are envisaged – or are in the process of being implemented – that would modify the existing situation;
- provide information about all abbreviations and terms used;
- indicate when questions are not applicable and explain how it came to this conclusion.

1.4 STATISTICAL INFORMATION

The GA should report the following information to the national central bank (NCB) of the country where it is legally incorporated or, where otherwise agreed, to the European Central Bank (ECB):

- general statistical information about the CPS;
- statistical information regarding fraud encountered by the scheme during the reporting period.

For further details, please refer to the "Reporting requirements for aggregated statistics on card payment schemes".

1 For examples of contractual agreements, scanned copies showing the date and signatures need to be provided. Specific information such as the amount of an agreed fee can be blacked out.

1.5 INFORMATION REGARDING INCIDENTS

"Incident reporting" concerns major incidents. Such incidents should be reported to the overseeing NCB (or the ECB) immediately. An incident should be classified as "major" if it has caused significant business disruption or interrupted the smooth functioning of the CPS or one of its sub-systems described in Annex 1 of the "Card payment scheme oversight framework – standards". For example, any major network failure or a major fraud incident involving CPS data should be reported.

For further details, please refer to the information that will be provided separately.

2 GENERAL INFORMATION REQUIRED FROM CARD PAYMENT SCHEMES

2.1 ESTABLISHMENT OF THE CARD PAYMENT SCHEME

The CPS indicates its GA, the place of incorporation of the GA and the legal status of the GA. The CPS states whether there are different GA entities for its business (e.g. for its euro area business and for its global business) and provides sufficient information about their roles and responsibilities. The CPS indicates the GA entity responsible for its euro area business.

The following documents and information could be of relevance:

- *the GA's form of incorporation (i.e. whether the CPS is a non-profit organisation, a corporation, a publicly listed company, etc.);*
- *the GA's registration in a commercial register and/or competent authorities' public registers (e.g. supervisory licensing), the effective date of these registrations and information about valid licences and authorisations granted or documents clarifying the status of the GA;*
- *a copy of the articles of association;*
- *information about the GA's registered branches and subsidiaries which are of relevance for the CPS's business; extracts from the relevant commercial and public registers; the functions and responsibilities of the branches/subsidiaries;*
- *a list of shareholders/partners and their shares/equity interests.*

2.2 CARD PAYMENT SCHEME BUSINESS OVERVIEW

The GA should provide a description of how the CPS functions, including a graphical overview of the main actors and processes. This overview should clearly show all of the CPS's outsourced functions.

The following documents and information could be of relevance:

- *description of the CPS's business activities for the euro area, the Single Euro Payments Area (SEPA) and worldwide;*

– *information about the shares of the transactions being carried out (e.g. the share of transactions directly conducted by the GA or the share of transactions where independent PSPs are involved) for the last three years of business;*

– *information about interactions between the CPS and other CPSs, PSPs, payment systems and/or other types of financial market infrastructure (e.g. business processes, graphical presentations and explanatory descriptions, descriptions of the services used/performed, etc.) and information on the business model(s) for these interactions (e.g. agreements, contractual terms and conditions, etc.).*

2.3 STRUCTURE OF THE CARD PAYMENT SCHEME

The GA should provide a clear and unambiguous description of the nature of the relationships between the GA, shareholders and network participants.

The following documents and information could be of relevance:

– *role, functions and responsibilities of the GA; the CPS's management structure (e.g. head office and location(s) where the CPS's actual management occurs with regard to its functions and main processes), as well as a list of people managing and representing the GA and of the members of its management and supervisory bodies;*

– *main rules on the governance and management of the CPS; information about the CPS's payment service providers, technical service providers as well as clearing and settlement providers, and information on their roles, functions and responsibilities;*

– *the CPS's organisational chart, encompassing all of the CPS's business activities, processes and functions and including any other entity performing the governance functions for the CPS and outsourcing service providers, as well as an explanatory description of the organisational chart.*

2.4 ACCESS CRITERIA

The GA should formulate the CPS access and exit criteria with sufficient levels of objectivity.

The following documents and information could be of relevance:

– *information on the conditions to be met to adhere to or exit (i.e. termination criteria) from the scheme and the different access criteria applied;*

– *information on the conditions to be met to become an issuer, acquirer, cardholder, card acceptor, technical service provider, clearing provider or settlement provider;*

– *exhaustive and up-to-date list of the PSPs participating in the CPS, as well as clearing and settlement providers.*

2.5 AUTHORISATION, CLEARING AND SETTLEMENT

The GA should describe the authorisation process and the clearing and settlement mechanisms used by the CPS and its actors to process the clearing and settlement of transactions for its different brands.

The following documents and information could be of relevance:

- *information on the different transaction phases and the related security measures (e.g. strong customer authentication methods);*
- *information on the entities involved in the authorisation services;*
- *information on the entities involved in the clearing services;*
- *information on the entities involved in the settlement arrangements;*
- *whenever applicable, an indication of the use of interbank and on-us transactions and correspondent banking;*
- *information on the functions of the GA or of other CPS actors related to clearing and/or settlement; a description of how clearing and settlement take place (e.g. for transactions within a euro area country; for intra-euro area cross-border transactions; for cross-border transactions between EU Member States where one counterparty is situated outside the euro area, etc.);*
- *information about the level at which the netting of euro area transactions takes place (e.g. per bank, national, EMEA (Europe, the Middle East and Africa), etc.).*

2.6 OUTSOURCING

The GA should provide information about important outsourcing service providers used and the functions for which they are used.

The following documents and information could be of relevance:

- *lists of outsourcing service providers, as well as the services and functions for which third parties are being used and the responsibilities and functions entrusted to them.*

2 OVERSIGHT ASSESSMENT QUESTIONS FOR CARD PAYMENT SCHEMES AND OVERSIGHT GUIDELINES

1 THE CARD PAYMENT SCHEME SHOULD HAVE A SOUND LEGAL BASIS UNDER ALL RELEVANT JURISDICTIONS

1.1 LEGAL FRAMEWORK

THE LEGAL FRAMEWORK GOVERNING THE ESTABLISHMENT AND FUNCTIONING OF A CARD PAYMENT SCHEME AND THE RELATIONSHIP BETWEEN THE SCHEME AND ITS ISSUERS, ACQUIRERS, CUSTOMERS AND SERVICE PROVIDERS SHOULD BE COMPLETE, UNAMBIGUOUS, UP-TO-DATE, ENFORCEABLE AND COMPLIANT WITH THE APPLICABLE LEGISLATION.

ESTABLISHMENT AND FUNCTIONING OF THE CARD PAYMENT SCHEME

1.1.1 SCHEME ESTABLISHMENT

Are the rules governing the establishment and functioning of the GA compatible with the applicable national and EU legislation? Does the GA perform regular/event-driven reviews of that compatibility?

- The jurisdiction/law governing the establishment of the GA is clearly identified.
- The GA has sought legal advice (e.g. from internal/external lawyers, competent authorities) about the compatibility of the rules governing its establishment and functioning with the applicable national and EU legislation (e.g. commercial law, consumer protection law, financial regulation, competition law, data privacy legislation, transparency requirements, etc.).
- The GA ensures that the results of the legal advice are properly taken into account.
- The GA has procedures in place ensuring regular/event-driven reviews of that compatibility (e.g. after critical court cases, changes of applicable law, etc.).
- The GA has the ability to take measures to maintain a sound legal basis for the CPS and has done so when needed.

Background documents and information:

- *the CPS's rules governing its establishment and functioning;*
- *jurisdiction/law governing the establishment of the GA and the operation of the CPS (for its business in the euro area/EU and for its business worldwide);*
- *information on legal advice received and the quality thereof;*
- *most recent compatibility review of the rules governing the establishment and functioning of the CPS (e.g. results, follow-up actions, experience gained, changes implemented, etc.);*
- *organisational role and responsibilities of the GA's internal legal function (if there is one) and the responsibilities of any external/independent lawyers providing legal advice;*
- *information on the measures taken by the GA to maintain a sound legal basis for the CPS (e.g. monitoring of legal developments, etc.).*

1.1.2 COMPLIANCE WITH LEGISLATION

Are the rules and procedures of the CPS compliant with all legislation specifically applicable to card payments and/or the processing of card payments? Does the GA perform regular/event-driven reviews of this compliance?

- The GA has sought legal advice (e.g. from internal/external lawyers, competent authorities) about the compliance of CPS rules with specific legislation (e.g. the Payment Services Directive (PSD), the Regulation on interchange fees for card-based payment transactions, anti-money laundering legislation[1]) relating to card payments and/or to the electronic processing of payments in the countries where the CPS is operating.

- The GA ensures that the results of the legal advice are properly taken into account.

- The GA requires the CPS's service providers[2] to check the compliance of their own rules and procedures with the legislation applicable to them and to ensure, where necessary, the validation beforehand by a competent authority of instructions regarding the customer's responsibilities.

Background documents and information:

  – *the CPS's rules and procedures for card payments and/or the processing of card payments;*

  – *compliance assessment of the CPS's rules and procedures with all legislation applicable to card payments and/or to the electronic processing of payments in the countries where the CPS operates;*

  – *information on legal advice received;*

  – *most recent legal compliance review (e.g. results, follow-up actions, experience gained, changes implemented, etc.);*

  – *the CPS's policies and procedures requiring the CPS actors to check the compliance of their own rules and procedures with the legislation applicable to them.*

1.1.3 COMPLETENESS, UNAMBIGUITY AND ENFORCEABILITY

Is it regularly ensured that all of the CPS's applicable rules and procedures are complete, unambiguous and enforceable?

- The GA has procedures in place to regularly ensure that the CPS's rules and procedures that it has set are complete, unambiguous and enforceable at least in terms of the following:

  – every new service/facility is included in all relevant rules and procedures prior to its operational implementation (completeness);

1 For example, Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, pp. 15-36. See also Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis, OJ L 214, 4.8.2006, pp. 29-34.

2 For the definition of service providers, please refer to the glossary.

- complaints from actors on the interpretation of the documentation and procedures are checked and addressed (unambiguity);

- rules and procedures are enforceable on each contractual party in accordance with the legislation applicable locally to the contract (enforceability).

- The GA requires that rules and procedures set by the CPS's service providers are compliant with the ones set by the GA and that they are complete, unambiguous and enforceable.

Background documents and information:

- *information on procedures used to check on a regular/event-driven basis the rules and procedures of the CPS for completeness, unambiguity and enforceability;*

- *information on the most recent review of the CPS's rules and procedures (e.g. results, follow-up actions, experience gained, changes implemented, etc.);*

- *the CPS's policies ensuring that the rules and procedures set by the CPS service providers are compliant with the ones set by the GA and that they are complete, unambiguous and enforceable;*

- *complaints from CPS actors on the interpretation of the documentation and procedures over the last two years (e.g. number of complaints, major issues, follow-up actions, etc.);*

- *information on any recommendations, follow-up actions, experience gained, changes implemented, outcomes, etc.*

CPS ACTORS' RELATIONSHIPS

1.1.4 LEGALLY BINDING NATURE

Are the relationships between CPS actors governed by specific and legally binding contractual arrangements? Do such arrangements cover all functions performed by CPS service providers, including any that are spread over different geographical areas?

- The GA requires CPS service providers to ensure that:

  - *the relationships between CPS actors in the different countries are contractually documented;*

  - *these contracts are signed and legally binding under the different laws of the countries where the CPS is operating.*

- The GA has a procedure in place to ensure that all the functions performed by CPS service providers, including any that are spread over different geographical areas, are covered.

Background documents and information:

- *contractual arrangements which govern the relationships between CPS actors, including information on the applicable laws;*

– *description of any material legal issues with regard to specific contractual provisions under the different jurisdictions where the CPS operates;*

– *information on procedures established to ensure that the relevant jurisdiction/law is taken into account in the contractual arrangements governing the relationships between CPS actors.*

1.1.5 ACTORS

Are the relationships/contractual arrangements between CPS actors compliant with the applicable national and EU legislation? Do all CPS service providers perform regular/event-driven reviews of that compatibility?

- The GA has sought legal advice (e.g. from internal/external lawyers, competent authorities) about the compatibility of relationships/contractual arrangements with CPS actors with national and EU legislation (e.g. commercial law, consumer protection law, financial regulation, competition law, data privacy legislation, transparency requirements, etc.).

- The GA ensures that the results of the legal advice are properly taken into account.

- The GA requires the CPS service providers to check the compliance of their own relationships/ contractual arrangements with the legislation applicable to them.

Background documents and information:

– *applicable national and EU legislation;*

– *measures taken by the GA to check whether CPS service providers act accordingly;*

– *information on the most recent legal advice received to test and ensure that the provisions of the contractual arrangements between CPS actors are compatible with national and EU legislation;*

– *information on any recommendations, follow-up actions, experience gained, changes implemented, outcomes, etc.*

1.1.6 COMPLETENESS, UNAMBIGUITY AND ENFORCEABILITY AMONG ACTORS

Is it ensured on a regular/event-driven basis that contractual arrangements between CPS actors are complete, unambiguous and enforceable?

- The GA has procedures in place to ensure on a regular/event-driven basis that contractual arrangements between the GA and other CPS service providers (and in case of three-party schemes between the GA and customers) are complete, unambiguous and enforceable at least in terms of the following:

  – all actors can operate under a valid contractual agreement, which will be adapted if need be (completeness);

  – contracts are signed by the relevant parties;

- complaints from actors on the interpretation of the documentation and procedures are checked and addressed (unambiguity);

- contractual provisions are enforceable on each contractual party in accordance with the legislation applicable locally to the contract (enforceability), including certification by competent authorities where applicable.

- The GA requires that contractual arrangements concluded by CPS service providers are compliant with the rules and procedures set by the GA and that they are complete, unambiguous and enforceable.

Background documents and information:

- *policies and procedures implemented to ensure that the contractual arrangements set by the CPS service providers are compliant with the rules and procedures set by the GA and that they are complete, unambiguous and enforceable;*

- *complaints from CPS actors on the interpretation of the documentation and procedures over the last two years (e.g. number of complaints, major issues, follow-up actions, etc.).*

1.2 JURISDICTIONS GOVERNING THE OPERATIONS OF THE CARD PAYMENT SCHEME

WHERE DIFFERENT JURISDICTIONS GOVERN THE OPERATION OF THE SCHEME, THE LAW OF THOSE JURISDICTIONS SHOULD BE ANALYSED IN ORDER TO IDENTIFY THE EXISTENCE OF ANY CONFLICT. WHERE SUCH CONFLICT EXISTS, APPROPRIATE ARRANGEMENTS SHOULD BE MADE TO MITIGATE THE CONSEQUENCES OF SUCH CONFLICT.

1.2.1 GOVERNING LAWS, COMPETENT COURTS

Are the governing law(s) and the competent court(s) which are applicabe to the relationships among CPS actors clearly identified?

- The GA has a procedure in place to identify the different jurisdictions related to CPS contractual arrangements.

- The GA requires the CPS service providers to have similar procedures in place and to act accordingly.

Background documents and information:

- *procedures established to identify the different jurisdictions related to CPS contractual arrangements;*

- *most recent legal advice received on contractual arrangements between CPS actors in order to identify jurisdictions and governing laws;*

- *information on any recommendations, follow-up actions, experience gained, changes implemented, outcomes, etc.*

1.2.2 CONFLICTS OF LAW

Has the GA examined the question of whether potential conflicts of law, having the potential to significantly impact the scheme, could arise between the different jurisdictions where the scheme operates? Once the conflicts have been identified or have materialised, what are the measures taken in order to mitigate the possible consequences of these conflicts?

- The GA has sought legal advice (e.g. from internal/external lawyers, competent authorities) in order to identify potential conflicts between these jurisdictions and to assess the potential impact on the scheme (e.g. by classifying these conflicts based on their likelihood and their impact).

- The GA ensures that the results of the legal advice are properly taken into account and mitigation measures (e.g. an insurance policy, a provision for legal risks, out-of-court conflict resolution procedures, etc.) have been put in place.

- The GA monitors the resolution of conflicts and requires CPS service providers to report possible conflicts of law that have the potential to significantly impact the scheme.

Background documents and information:

  – *legal advice received;*

  – *policy for mitigation and resolution of conflicts between jurisdictions;*

  – *arbitration clauses in contract templates.*

2 THE CARD PAYMENT SCHEME SHOULD ENSURE THAT COMPREHENSIVE INFORMATION, INCLUDING APPROPRIATE INFORMATION ON FINANCIAL RISKS, IS AVAILABLE TO THE ACTORS

2.1 RULES AND CONTRACTUAL ARRANGEMENTS

ALL RULES AND CONTRACTUAL ARRANGEMENTS GOVERNING THE CARD PAYMENT SCHEME SHOULD BE ADEQUATELY DOCUMENTED AND KEPT UP TO DATE. ALL ACTORS AND POTENTIAL ACTORS SHOULD BE ABLE TO EASILY ACCESS INFORMATION RELEVANT TO THEM, TO THE EXTENT PERMITTED BY DATA PROTECTION LEGISLATION, SO THAT THEY CAN TAKE APPROPRIATE ACTION IN ALL CIRCUMSTANCES. SENSITIVE INFORMATION SHOULD ONLY BE DISCLOSED ON A NEED-TO-KNOW BASIS.

2.1.1 ROLES AND RESPONSIBILITIES

Are the roles and responsibilities derived from the rules and contractual arrangements for CPS actors clearly documented and updated on a regular/event-driven basis?

- The GA holds a complete set of documentation related to the adherence to and the governance and functioning of the CPS.
- This documentation describes the roles and responsibilities of all actors and includes information on the secure use of the service.
- The documentation is updated on a regular/event-driven basis (i.e. at least in case of changes).

Background documents and information:

- *the CPS's rules and contractual arrangements related to the governance and functioning of the CPS;*
- *information on the roles and responsibilities of all CPS actors, as derived from the rules and contractual arrangements;*
- *information on the procedures implemented to update the set of rules and contractual arrangements governing the CPS on a regular/event-driven basis (at least in case of changes).*

2.1.2 DISCLOSURE POLICY

Is relevant information easily available to actors and potential actors (sensitive information should only be disclosed on a need-to-know basis and in accordance with the relevant data protection legislation)? Are major changes (e.g. regarding technical features, financial aspects or the security policy for devices such as cards and terminals) within the scheme announced to actors well in advance?

- The GA has defined a classification procedure for information based on its sensitivity.
- Disclosure of information to all actors or potential actors is based on this classification and their need to know. This information is made available via different and appropriate communication channels (i.e. in a safe and trusted environment for sensitive information or, if communicating

through alternative channels such as SMS, e-mail or letter, sensitive data should either be masked or not included) at an acceptable frequency.

- The GA has a procedure to ensure that the information is clear and easily understandable (e.g. no major complaints from actors) and for monitoring major complaints in this respect.

- The GA has a procedure ensuring that:

  – all actors are informed about major changes relevant to them (e.g. through a consultation of relevant actors prior to implementation);

  – in case of consultations, the final decisions are made available to the relevant actors (e.g. via websites, circulation of letters);

  – all actors have enough time to prepare themselves for the major changes.

- There are clear responsibilities within the CPS for the announcement/communication of major changes.

Background documents and information:

  – *procedures for the classification of information based on its sensitivity and disclosure rules;*

  – *rules and procedures established for informing actors about major changes (e.g. notice periods, terms and conditions);*

  – *complaints from the actors over the last two years (e.g. number of complaints, major issues, follow-up actions, mitigation measures taken, final outcomes and lessons learned).*

2.1.3 FEES

Are the fee structures and fees for the services received clearly documented and made available to all relevant actors as well as to potential actors during the contractual negotiation process?

- The GA produces and requires PSPs to produce detailed statements about fee structures and fees (e.g. member access and annual fees, interchange fees, end-user fee policy, etc.), which are disclosed to all relevant actors and to potential actors during the contract negotiation process.

Background documents and information:

  – *fee structures and fees for services;*

  – *information on the disclosure process.*

2.2 ACCESS TO RELEVANT INFORMATION

ISSUERS, ACQUIRERS, CARDHOLDERS AND CARD ACCEPTORS SHOULD HAVE ACCESS TO RELEVANT INFORMATION IN ORDER TO EVALUATE FINANCIAL RISKS AFFECTING THEM.

2.2.1 INFORMATION ON FINANCIAL RISKS

Is relevant information available to current and potential actors to enable them to evaluate the financial risks affecting them?

- The GA provides current and potential issuers and acquirers with sufficient information in order to evaluate potential financial risks relevant for them and requires them to disclose the relevant information to current and potential customers.

- This information includes descriptions of any liabilities and obligations that determine the allocation of financial risk (including basic information concerning the use and abuse of cards and terminals as well as conditions and liabilities).

- Where appropriate this information is easily understandable (e.g. there have been no major complaints from the actors) and available (e.g. via different communication channels and in the terms and conditions).

- The GA has a procedure for monitoring major complaints in this respect.

Background documents and information:

  – *description of the information provided to current and potential actors in order to evaluate potential financial risks relevant to them;*

  – *the CPS's overview of the different financial risks (e.g. types, estimates of the magnitude of their impact, etc.) that current and potential actors would face;*

  – *information on the complaints from actors over the last two years (e.g. number of complaints, major issues, follow-up actions, mitigation measures taken, final outcomes and lessons learned).*

2.2.2 CHARGE-BACK AND FRAUD INFORMATION

Is sufficient and up-to-date information on fraud and its mitigation (e.g. on recognising skimming devices and protecting PINs or other cardholder authentication methods) available to actors and also to potential actors? Is the security awareness of customers maintained and improved in line with their responsibilities and liability?

- The GA has set general rules for PSPs to inform their customers about the use of card payments (e.g. limits for the payment services provided, possibility to disable the internet payment functionality).

- The GA either implements or requires PSPs to have a security awareness programme that ensures that customers understand the need to:

  – protect sensitive payment data (e.g. their passwords, security tokens, personal details and other confidential data);

  - manage properly the security of their personal device (e.g. computer) by installing and updating security components (e.g. antivirus, firewalls, security patches);

  - consider the significant threats and risks related to downloading software via the internet if the customer cannot be reasonably sure that the software is genuine and has not been tampered with;

  - use the genuine website of the issuer or acquirer.

- This security awareness programme is relevant, complete (e.g. it includes customer feedback loops in order to measure its effectiveness, i.e. important messages are understood by the recipients, and its reach, i.e. number of clients), easily accessible and understandable for the customer.

- The GA requires that PSPs have explained: (i) the procedure for customers to report (suspected) fraudulent payments, suspicious incidents or anomalies, including during the internet payment services session and/or possible social engineering attempts; (ii) how the PSP will respond to the customer; and (iii) how the PSP will notify the customer about (potential) fraudulent transactions or their non-initiation, or will warn the customer about the occurrence of attacks (e.g. phishing e-mails).

- The GA requires PSPs to have a procedure to ensure that customers are informed through a secure channel about updates to security procedures and any alerts about significant emerging risks (e.g. warnings about social engineering).

- In case of charge-backs, fraud activities and mitigation measures, the GA ensures that all relevant actors are involved.

Background documents and information:

  - *fraud prevention measures, reporting and security policy;*

  - *fraud data for the last 12 months (e.g. type of fraud, examples, etc.) and the relevant security issues;*

  - *follow-up actions, outcomes, conclusions, recommendations and advice taken;*

  - *security awareness programme documentation (e.g. leaflets, information material, feedback forms).*

In addition, the GA is encouraged to comply with the following best practices:

- The GA could require acquirers to:

  - offer physical or virtual educational programmes on fraud prevention; the content and documentation should be relevant and easily accessible;

  - prove that training programmes are attended on a regular basis by a significant number of card acceptors (i.e. a procedure is in place to track the number of merchants that attended courses and completed the programmes);

– define risk categories for card acceptors and ensure that high-risk card acceptors in particular are involved in the educational programmes.

2.2.3 CRISIS COMMUNICATION AMONG AFFECTED ACTORS

Are there provisions in place for communication between affected actors in crisis situations that have a financial impact?

- According to the risk analysis, the GA has defined appropriate communication provisions (e.g. a policy for service providers, communication channels, etc.) between actors which are financially affected due to significant disruptions in the functioning of a CPS.

- The GA requires that these provisions are followed by all service providers (e.g. in rules or service level agreements).

Background documents and information:

– *communication provisions for crisis situations involving a financial impact on actors.*

2.2.4 APPROPRIATE INFORMATION TO CARDHOLDERS

Are cardholders appropriately informed by their PSPs about preventive and corrective actions (e.g. handling of personal authorisation credentials)?

- The GA has set general rules for issuers with the aim of informing cardholders about the risks of participating in the scheme. This information should be easily understandable and available (e.g. via different communication channels and in the terms and conditions).

- The GA requires issuers to supply cardholders, prior to their entering into a contract for the provision of payment services, with the information outlined in the PSD ("Information and conditions"), including specific details relating to the use of card payments over the internet. These should include, as appropriate:

  – clear information on any requirements in terms of the cardholder's equipment, software or other necessary tools (e.g. antivirus software, firewalls);

  – guidelines for the proper and secure use of personalised security credentials;

  – a step-by-step description of the procedure for the cardholder to submit and authorise a payment transaction and/or obtain information, including the consequences of each action;

  – guidelines for the proper and secure use of all hardware and software provided to the cardholder;

  – the procedures to be followed in the event of loss or theft of the personalised security credentials or the cardholder's hardware or software for logging in or carrying out transactions;

  – the procedures to be followed if abuse is detected or suspected;

  – a description of the responsibilities and liabilities of the issuer and the cardholder with regard to the use of card payments over the internet.

- The GA requires issuers to obtain from cardholders a formal acknowledgement of the receipt of this information.

- The GA requires that issuers include clauses in their contracts with their cardholders related to the blocking of specific transactions or the payment service on the basis of security concerns. These contracts should at least specify:

  – the payment modalities;

  – the retry limits for authentication;

  – the procedure to be followed to reactivate the payment service;

  – the communication modalities between the cardholder and the issuer for unblocking a blocked service.

- The GA requires the issuers to:

  – inform cardholders of at least one secure channel (e.g. online banking, encrypted and digitally signed e-mail, dedicated secure website, ATM) for ongoing communication with cardholders regarding the correct and secure use of payment cards, including over the internet, and explain that any message on behalf of the PSP via any other means, such as e-mail, which concerns the correct and secure use of the payment service, is not reliable. This procedure is implemented in practice (e.g. in the customer contracts, in customer information leaflets, in information campaigns or on websites);

  – have a procedure in place communicating how cardholders can obtain assistance. This might include initial information when signing the contract, indications on the PSP's website, emergency numbers or authentication tools;

  – inform the cardholders in a transparent way that they may disable the internet payment functionality. The relevant procedure is efficient and clearly explained;

  – inform the cardholders that they may register for strong authentication irrespective of a specific card payment transaction over the internet. Issuers should actively encourage cardholders to enrol for strong authentication and to allow cardholders to bypass such an enrolment only in exceptional and in a limited number of cases;

  – establish a procedure for providing information to cardholders which is appropriate, secure and not misleading. This procedure should be clearly explained to cardholders, including all relevant aspects (e.g. when changes of limits become effective).

Background documents and information:

  – *scheme rules on secure communications;*

  – *external audits.*

In addition, the GA is encouraged to comply with the following best practice:

- The GA could require issuers to offer dedicated service contracts for conducting internet payment transactions. Where necessary, these dedicated service contracts have been validated beforehand by a competent authority.

2.2.5 INFORMATION ON RISKS TO CARD ACCEPTORS

Are card acceptors made aware of the risks they face as a consequence of participating in the scheme?

- The GA has set general rules for acquirers with the aim of informing card acceptors about the risks of participating in the scheme. This information should be easily understandable and available (e.g. via different communication channels and in the terms and conditions).

- The GA requires acquirers to supply card acceptors, prior to their entering into a contract for the provision of payment services, with the information outlined in the PSD ("Information and conditions"), including specific details relating to the use of card payments over the internet. This should include, as appropriate:

  – clear information on any requirements in terms of card acceptors' equipment, software or other necessary tools (e.g. antivirus software, firewalls);

  – guidelines for the proper and secure use of personalised security credentials;

  – guidelines for the proper and secure use of all hardware and software provided to the card acceptor;

  – the procedures to be followed in the event of loss or theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions;

  – the procedures to be followed if abuse is detected or suspected;

  – a description of the responsibilities and liabilities of the acquirer and the card acceptor with regard to the use of card payments over the internet.

- The GA requires acquirers to obtain from card acceptors a formal acknowledgement of the receipt of this information.

- The GA requires acquirers to have a procedure in place determining how the card acceptors can obtain assistance. This might include initial information when signing the contract, indications on the PSP's website, emergency numbers for payment instruments or authentication tools.

Background documents and information:

  – *list of the rules set to inform card acceptors about the risks of participating in the scheme.*

3 THE CARD PAYMENT SCHEME SHOULD ENSURE AN ADEQUATE DEGREE OF SECURITY, OPERATIONAL RELIABILITY AND BUSINESS CONTINUITY

3.1 SECURITY MANAGEMENT

3.1.1 AN ANALYSIS OF OPERATIONAL AND SECURITY RISKS SHOULD BE CONDUCTED ON A REGULAR BASIS IN ORDER TO DETERMINE THE ACCEPTABLE RISK LEVEL AND SELECT ADEQUATE SECURITY POLICIES AND APPROPRIATE PROCEDURES IN ORDER TO PREVENT, DETECT, CONTAIN AND CORRECT SECURITY VIOLATIONS. COMPLIANCE WITH SUCH SECURITY POLICIES SHOULD BE ASSESSED ON A REGULAR BASIS.

3.1.1.1 RISK ANALYSIS

Is a comprehensive risk analysis conducted by the GA and updated on a regular/event-driven basis, taking into account all the different risk profiles of the various CPS actors? Does the GA ensure that all organisational, personnel, infrastructural and technical issues are dealt with and that the necessary security policies have been selected?

- The GA carries out and documents a reproducible risk analysis based on up-to-date risk management methodologies that are recognised industry-wide (e.g. risk management methodologies developed by ISO, the Project Management Institute or the National Institute of Standards). This risk analysis is carried out using qualitative and/or quantitative methods, i.e. risks are expressed in financial terms or by level (e.g. significant, major, etc.).

- The risk analysis deals with all aspects relevant to the functioning of the CPS (e.g. organisational, personnel, infrastructural and technical issues, possible security threats (internal and external) and their magnitude (impact and likelihood), existing or potential safeguards (e.g. technical controls, insurance)). It includes a detailed risk analysis of the operational functions of the scheme (e.g. manufacturing of cards and accepting devices, issuance of cards, operation of accepting devices, communication network facilities, acquiring of transactions, clearing and settlement). It takes into account the technological solutions and platforms used, the application architecture, the programming techniques and routines, as well as all payment channels.

- The GA has defined a procedure to review and update the risk analysis, as well as to reflect the results in the security policies and specifications.

- The GA requires CPS service providers to conduct their own risk analyses and to report issues of scheme-wide importance to the GA.

  Background documents and information:

  – *risk analysis and the procedures defined by the GA for reviewing and updating it;*

  – *rules of the GA for CPS service providers regarding their risk analysis and the reporting of issues.*

3.1.1.2 SECURITY POLICIES AND SERVICE LEVELS

Do the security policies define the objectives and the organisation of information security? Does the GA monitor and assess whether security policies and operational service levels are met within the CPS? Is this a continuous and comprehensive process?

(Clearing and settlement arrangements and systems which are already covered by oversight are excluded.)

- The GA has documented operational service levels and security policies covering the appropriate domains (e.g. security management, protection of sensitive data or devices during manufacturing, distribution of cards, initiation and processing of transactions, clearing and settlement, business continuity and outsourcing) including those relevant to the use of card payments over the internet.

- The security policies define at least the following elements:

  – objectives and organisation of information security (including a reference to internet payment services);

  – principles for the secure use and management of information, as well as information and communication technology (ICT) resources;

  – roles and responsibilities, as well as security activities and processes.

- The security policies include a risk assessment, with particular reference to control and mitigation activities concerning the management of sensitive payment data:

  – human resource security;

  – information security across the organisation (e.g. the risk management function[1]);

  – logical/physical security controls;

  – security arrangements for information/services outsourced.

- The GA has put in place a process for making the relevant parties aware of the security policies and procedures, and for assessing the implementation of the CPS's operational service levels, security policies as well as other requirements linked to security.

- If this assessment does not encompass the implementation of the operational service levels of the service providers operating in the scheme and the security policies, the GA requires those service providers to assess whether the implementation of their own operational service levels and security policies is of an acceptable level (e.g. via contracts).

- The assessment(s) of the implementation of the operational service levels and the security policies is a continuous (i.e. at least once a year) and comprehensive process (i.e. it covers all

1 i.e. coordinated activities to direct and control the organisation with regard to risk; it typically includes risk assessment, risk treatment, risk acceptance and risk communication.

the functions of the CPS[2] and encompasses the review of the impact of major incidents and major changes).

- With reference the GA's security policy sections that are applicable to all payment scheme service providers, the GA has defined requirements and/or contractual agreements which require all payment scheme service providers to comply with the GA's security policy (e.g. scheme rules provisions). For all other aspects, the GA requires service providers to have their own security policies in place.

  Background documents and information:

  – *CPS's security policies and procedures;*

  – *CPS's security monitoring framework;*

  – *information on the process for assessing the implementation of the CPS's security policies, operational service levels and other requirements linked to security;*

  – *list of the relevant controls performed (including external audits) and recommendations issued over the last two years.*

In addition, the GA is encouraged to comply with the following best practice:

- The GA could lay down the security policy for internet payments in a dedicated document and require CPS service providers to do the same.

3.1.1.3 FORMAL APPROVAL AND DOCUMENTATION

Is the security policy in line with the risk analysis? Does it include residual risks? Are both approved by the Board? Is there a direct reporting line between the risk manager and the Board?

- The GA ensures that the security policy considers the risk analysis and mitigates risks according to its risk appetite (capacity to absorb financial losses, reputational damage, etc.).

- The security policy and the residual risks have been approved by the Board or an adequate management body, communicated and made available on a need-to-know basis to all relevant employees and external parties.

- The security policy defines clear reporting lines between the risk manager and the Board.

  Background documents and information:

  – *security policy;*

  – *board approval of the security policy and residual risk accepted.*

2 It is also acceptable not to cover all functions at the same time, but to review them following a cyclical pattern.

3.1.1.4 MONITORING OF DEVELOPMENTS

Does the GA monitor new developments in technology and security and reassess the level of threats and vulnerabilities accordingly in order to adapt the security policies of the CPS? Are rules in place requiring CPS service providers to inform the GA about any technological developments that have a significant impact on the scheme?

- The GA has documented the criteria that drive the review and updating of the security policies:
  - the security policy review is carried out at least once a year on the basis of a formal and well-documented procedure. The procedure clearly defines:
    a) the frequency and criteria for its activation (e.g. major changes in the risk assessment results, in the business models or in the technologies adopted), the role and responsibilities of entities involved, and the time schedule for its execution;
    b) inputs for the review (e.g. risk assessment results, audit results, effective measurements and status of corrective actions, recommendations from authorities, any changes that could affect payment services, including internet payment services, etc.);
    c) review outputs (e.g. overview of threats and vulnerabilities, risk treatment and remedial action plan, resource needs, etc.);
  - the results of the reviews are clearly documented and records are maintained.
- The GA monitors technological developments relevant for the functioning and security of the CPS, especially with regard to fraud techniques (both for internal and external fraud) and the evolution of the characteristics and features of the instrument and the initiation channels, and takes remedial actions.
- The GA requires all CPS service providers (e.g. via contracts) to:
  - monitor new technological development themselves, especially with regard to fraud techniques and the evolution of the characteristics and features of the instrument and the initiation channels;
  - report to the GA information of scheme-wide importance gained from their own monitoring of technological developments.

Background documents and information:

- *list of criteria for updating the security policy;*
- *details of the last review of the security policy;*
- *contracts signed with the service providers.*

3.1.2 MANAGEMENT AND STAFF SHOULD BE TRUSTWORTHY AND FULLY COMPETENT (IN TERMS OF SKILLS, TRAINING AND NUMBER OF STAFF) TO MAKE APPROPRIATE DECISIONS, ENDORSE SECURITY POLICIES AND CARRY OUT THEIR CPS-RELATED RESPONSIBILITIES AND DUTIES

3.1.2.1 STAFF AWARENESS

Is it ensured that staff and management are aware and regularly reminded of the responsibilities and duties incumbent upon them given their documented role within the CPS?

- The responsibilities and duties of staff and management of the GA are well-documented and kept up to date (e.g. by means of an organisational chart, task descriptions, procedures, intranet, fraud prevention). The security roles and responsibilities of employees, contractors and third-party providers are defined and documented in accordance with the organisation's information security policy. For example, operational, contingency and control procedures clearly indicate the duties and responsibilities of staff and management. The documentation is relevant and easily accessible.

- The security roles and responsibilities include the requirement to:

  – implement and act in accordance with the security policies;

  – protect assets from unauthorised access, disclosure, modification, destruction or interference;

  – execute particular security processes or activities;

  – ensure responsibility is assigned to the individual for actions to be taken;

  – report actual or potential security events or other security risks to the organisation;

  – monitor new developments in technology and security (e.g. through participation in special security forums and professional associations) as well as review the security policies accordingly.

- The GA requires all CPS service providers (e.g. via contracts) to document the roles and responsibilities of their staff and management.

  Background documents and information:

  – *CPS operational, contingency and control procedures.*

3.1.2.2 STAFF TRUSTWORTHINESS

Is it ensured that sensitive operational activities (e.g. the management of cryptographic keys) are performed only by trustworthy staff?

- The GA has identified its sensitive operational activities. This information is kept up to date.

- The GA has defined access policies for sensitive operational activities.

- The GA performs a security investigation before hiring staff that will be performing sensitive operational activities, and requires that contracts with personnel include confidentiality clauses.
- The GA has identified its personnel authorised to perform these activities and has defined access rights accordingly.
- The GA requires CPS service providers to do the same.

  Background documents and information:

  – *confidentiality clauses included in contracts with personnel;*

  – *access policies for sensitive operational activities;*

  – *hiring policies and procedures for staff and management.*

3.1.2.3 STAFF COMPETENCE

Is it ensured that staff and management have and maintain the competences, skills and resources required to carry out their tasks?

- The GA has a process in place to identify and regularly review competences, skills and resources necessary for its staff and management to carry out their tasks. Related training (e.g. physical or virtual education programmes) is regularly updated to ensure that the content remains relevant to a dynamic security environment.
- The GA requires CPS service providers to identify and regularly review the competences, skills and resources necessary for their staff and management.

  Background documents and information:

  – *job descriptions and training plans;*

  – *information on the number of staff holding a valid industry certificate (e.g. CISSP, etc.);*

  – *staff appraisal policy and relevant templates.*

3.1.3 OPERATIONAL AND INCIDENT MANAGEMENT SHOULD BE CLEARLY DEFINED AND EFFECTIVELY IMPLEMENTED.

3.1.3.1 SCHEME MONITORING

Is it ensured that sufficient and up-to-date information on the status of systems, components, operational functions, administrative procedures, etc., is collected such that the CPS can manage its operations, security matters, incidents, fraud events, etc., effectively?

- The GA has defined the operational processes and equipment that are of particular importance for the functioning of the CPS. The GA collects sufficient and up-to-date information about these processes and equipment with the aim of monitoring their functioning and identifying early warnings of possible security incidents by detecting anomalies (e.g. the status of the

systems, components, operational functions, and administrative and technical procedures with regard to physical as well as information security incidents). This information includes incidents concerning operational reliability, security breaches and fraud.

- The GA requires the CPS service providers to do likewise for their own processes and equipment which are of particular importance for the functioning of their services.

  Background documents and information:

  – *operational processes and equipment of particular importance for the functioning of the CPS;*

  – *information on major incidents concerning operational reliability, security breaches and fraud over the last 12 months, follow-up actions, outcomes and lessons learned;*

  – *information on the procedures for operational and incident management;*

  – *audit reports and issued recommendations.*

3.1.3.2 INCIDENT MANAGEMENT

Are clear incident management and escalation procedures established and tested on a regular basis? Do they include a procedure for immediately notifying the competent authorities in the event of major payment security incidents, as well as for cooperating with the relevant law enforcement agencies?

- The GA has put in place, for the whole CPS, a system for classifying incidents and operational problems according to their criticality and for determining whether they need to be reported to the GA.

- The GA has defined incident management procedures (including escalation procedures, so that incidents which cannot be immediately resolved are appropriately escalated, both internally and externally to all CPS service providers), which are periodically reviewed and tested. These procedures include, when deemed relevant, clearly defined communication channels with all of the CPS service providers, so that incidents can be handled efficiently.

- The GA requires the CPS service providers to have incident management and escalation procedures in place, with clearly defined communication channels with the other CPS service providers and the GA (when deemed relevant). The GA requires that these procedures be periodically reviewed and tested.

- The GA has a procedure in place to immediately notify the competent authorities (i.e. supervisory, oversight and data protection authorities) in the event of major payment security incidents with regard to the payment services provided. This procedure defines how information is conveyed in a secure manner and how it is ensured that the respective contacts are up to date.

- The GA has a procedure in place to cooperate with the relevant law enforcement agencies on major payment security incidents, including data breaches. It has defined who is in charge, how information is conveyed in a secure manner and how it is ensured that the respective contacts are up to date.

- The GA requires acquirers to contractually require card acceptors that store, process or transmit sensitive payment data to cooperate with their PSP and the relevant law enforcement agencies on major payment security incidents, including data breaches.

- The GA requires PSPs to make available 24/7 customer assistance (e.g. online banking, hotline, e-mail) for notifications of anomalies or incidents regarding payments and related services and, during normal business hours, assistance for all questions, complaints and requests for support. CPS service providers have a procedure in place to ensure that, even if there is a major incident, appropriate information is communicated to customers.

  Background documents and information:

  – *information on the most recent review of the CPS's incident management and incident escalation procedures (e.g. results, follow-up actions, experience gained, changes implemented, etc.);*

  – *reports on incidents over the last 12 months (e.g. incidents registered, follow-up actions, escalation, outcomes, lessons learned, etc.);*

  – *audits and issued recommendations.*

3.1.3.3 INCIDENT FOLLOW-UP

Are major incidents and other relevant operational problems properly monitored and reported to the GA to allow them to be followed up and to ensure that they are resolved?

- The GA has put in place a procedure for the whole CPS to be informed about and to monitor and follow up on major incidents according to its classification (this information can include the logging/recording, notification, investigation, resolution and closure of problems).

- The GA requires that the contracts between all the actors include termination clauses in case of no cooperation on major payment security incidents.

- The GA requires service providers to have a procedure in place to monitor, handle and follow up on security-related customer complaints and report relevant results to the GA.

  Background documents and information:

  – *list of the major incidents and decisions made over the last two years;*

  – *proof of the information notified to competent authorities;*

  – *contracts*;

  – *report on security-related customer complaints and follow-up.*

3.1.3.4 CHANGE MANAGEMENT

Is a change management process in place for the whole CPS to ensure that changes are properly planned, tested, documented and authorised? Is this process regularly reviewed and updated?

- The GA has set up a formal change management process for requests for changes, including planning, testing, documenting and authorising changes, and appropriate communication channels with the CPS service providers concerned. The concept of major change is defined.

- The GA has set up procedures ensuring that there are clearly defined reasons for each change, that items affected by the change are properly identified, that changes are categorised, prioritised, documented, planned, tested and properly authorised before being implemented. A rollback plan is in place should the change result in unexpected negative consequences.

- The GA requires the CPS service providers to have similar procedures in place.

- The GA periodically reviews and updates the change management process, and communicates any changes to all CPS service providers affected. The GA requires the CPS service providers to do likewise and communicate major changes to the GA.

- The GA has a procedure in place ensuring that, before releases and changes go into production, relevant source codes are subject to code review by independent reviewers in order to minimise software vulnerabilities, backdoors and manipulation. It ensures that before going into production software releases and changes are subject to appropriate tests by testers other than the developers. It has controls in place to ensure appropriate documentation of any applications and IT systems. The GA requires service providers to comply with this procedure.

  Background documents and information:

  – *CPS change management policies and procedures;*

  – *information on the requests for changes over the last 12 months, including a description of the reasons for each change request, the items affected, and the relevant categorisation and prioritisation of these changes;*

  – *audits and issued recommendations.*

3.1.3.5 ACCESS POLICY

Are explicit and adequate policies defined to ensure that only those members of staff that have been assigned responsibility for supporting the CPS's business functions and operations have access (both logical and physical) to the required functions?

- The GA has identified the staff members responsible for the CPS's business functions and operations, and has restricted logical and physical access to these functions and operations (notably sensitive ones) to authorised staff only. The GA requires that CPS service providers have a similar identification and access policy in place.

- These requirements include that:

  – Access privileges (including for administrators, super users/roots, database administrators, etc.) associated with each system product (e.g. operating system, database management system and applications) and the users to which they need to be allocated should be identified and reviewed on a regular basis. Privileges should be allocated to users following the "least-privilege" principle[3] and, whenever feasible, on an event-by-event basis in line with the access control policy. An authorisation process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorisation process is complete. An effective recertification process for assessing and, if necessary, revoking privileges should be in place and carried out at regular intervals.

  – Appropriate processes should be in place to monitor, track and restrict logical and physical access to sensitive payment data and critical resources. Access is only given to authorised users and programs. Only authorised personnel have access to the log file evaluation tools and are able to parameterise them.

  – Administrative privileges should be assigned to users through a different user ID than the one used for normal business.

  Background documents and information:

  – *procedure for allocating/updating access privileges;*

  – *up-to-date list of staff and access privileges;*

  – *audits and issued recommendations.*

3.1.3.6 SEPARATION OF DUTIES

Is an appropriate separation of duties maintained (e.g. through the use of the "four-eyes" principle)?

- The GA's control functions are clearly distinguished from operational functions (e.g. quality checks are independent of the development process). All roles and responsibilities are clearly documented. This includes an appropriate separation of duties (e.g. management of secrets, access rights, authorisations, IT test and production environments, transfer of sensitive payment data to the development and test environments is avoided or, if necessary, temporarily allowed with specific control measures, etc.) at both the organisational and technical levels.

- The GA requires that all CPS service providers have equivalent control functions and procedures in place.

  Background documents and information:

  – *access policies and procedures.*

3 "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job." See Saltzer, J.H. (1974), "Protection and the Control of Information Sharing in Multics", *Communications of the ACM,* Vol. 17, No 7, p. 388.

3.1.4 THE CPS'S SECURITY POLICY SHOULD ENSURE PRIVACY, INTEGRITY AND AUTHENTICITY OF DATA AND CONFIDENTIALITY OF SECRETS (E.G. PIN) WHEN DATA ARE OPERATED, STORED OR EXCHANGED. IF SECRETS ARE REVEALED OR COMPROMISED, EFFECTIVE CONTINGENCY PLANS SHOULD BE IMPLEMENTED TO PROTECT THE CPS.

3.1.4.1 PROTECTION OF SENSITIVE PAYMENT DATA

Are sensitive payment data identified, managed and adequately protected? Where sensitive payment data are exchanged, is end-to-end encryption applied?

- The GA has a procedure to identify and list all elements it considers as sensitive payment data according to their protection needs and requires CPS service providers to have relevant controls to ensure the proper protection of sensitive payment data.

- The GA requires CPS service providers to ensure that data minimisation is an essential component of the core functionality during the design, development and maintenance phases (e.g. the service providers describe the protection measures put in place and outline both automated and manual controls that ensure that data minimisation is adhered to in the design, development and maintenance phases, so that the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive payment data achieved through the application are minimised).

- The GA has defined procedures to ensure the confidentiality of the authentication method when the authentication data are typed in at a terminal or other accepting device (e.g. point-of-sale terminal, ATM or mobile device), or sent from accepting devices to other CPS components. The GA requires all CPS service providers to comply with these procedures.

- The GA requires PSPs to ensure that all sensitive payment data accessible to customers online, for example through their e-banking websites or e-wallets, and the access to and/or amendment of these data, are protected with strong customer authentication. In case of consultative services with no display of sensitive customer or payment information, where alternative authentication measures are adopted, there is a risk analysis attached to those services to justify the adoption and the adequacy of such authentication solutions.

- The GA has set up or requires CPS service providers to set up specific procedures and technical measures, such as requiring tamperproof communication channels and secure authentication methods (e.g. VPN), to manage the servers or to use end-to-end encryption between the communicating parties[4] throughout the respective communication session (e.g. through the use of secure protocols, such as TLS) allowing mutual authentication according to current best practices (e.g. key length, TLS version, encryption cipher, etc.) in order to safeguard the confidentiality and integrity of the data. Strong and widely recognised encryption techniques, access control measures and audit trails are used to ensure that all sensitive payment data are appropriately secured against theft and unauthorised access or modification.

- The GA requires that card acceptors handling (i.e. storing, processing or transmitting) sensitive payment data are required by their PSP to implement security measures to protect such data in their IT infrastructure. These PSPs should encourage card acceptors not to store any sensitive payment data by offering services where the sensitive payment data would be under their responsibility.

4 The encryption should cover the whole communication session ("full session encryption").

- The GA has taken measures to enforce the contractual obligation (e.g. requiring acquirers to have set up a procedure to monitor compliance and to specify the steps to be taken in case of detected breaches) or terminate the contract.

  Background documents and information:

  – *policy on the protection and management of sensitive payment data;*

  – *contractual clauses that describe the requirements for managing sensitive payment data;*

  – *CPS procedures ensuring the confidentiality of authentication methods.*

In addition, the GA is encouraged to comply with the following best practice:

- The GA could require acquirers to ensure that, if card acceptors are handling sensitive payment data, they train their fraud management staff appropriately and update this training regularly to ensure that the content remains relevant to a dynamic security environment.

3.1.4.2 IT AND DATA SECURITY

Is there an appropriate IT and data security policy? Does it ensure the integrity of the IT system? Are the privacy, integrity and authenticity of data (including cardholders' personal data) and the confidentiality of secret information (e.g. credentials) maintained where such data are processed, stored and exchanged?

- The GA has appropriate security solutions in place and requires CPS service providers to have such solutions to protect networks, websites, servers and communication links against abuse or attacks, for example:

  – vulnerability scans and penetration tests run by certified auditors;

  – an effective patch management process in place that ensures that systems are in a sufficiently up-to-date patch state;

  – all critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of sensitive payment data by malicious individuals and software;

  – firewalls with appropriate rules to allow only legitimate connections;

  – measures to prevent or mitigate (distributed) denial of service attacks;

  – intrusion detection systems as well as intrusion prevention systems to signal and avert attacks identified by a heuristic analysis or by a known pre-set pattern;

  – controls in place to ensure the quality of the software architecture of relevant applications;

  – a policy in place to develop secure applications.

- The GA has requirements that the servers be stripped of all superfluous functions and unused services (hardening), including for example:
  - industry-accepted system hardening standards (e.g. CICS, ISP, SANS, NIST, etc.);
  - changing of user ID and credential defaults (e.g. administrators' passwords) before installing a product;
  - enabling only necessary services and protocols;
  - removal of all unnecessary functionality, such as scripts, drivers, features, sub-systems, file systems and unnecessary server applications.
- The GA has defined requirements ensuring that the privacy, integrity and authenticity of data are proportionate to their level of sensitivity and that the confidentiality of secret information (including at least the PIN) is maintained within the CPS during operation, storage and exchange (irrespective of the type of accepting device). More specifically and if relevant, the GA has defined a security policy for PIN creation, operation, distribution and storage.
- The GA tests and requires CPS service providers to test security measures for the use of card payments over the internet under the supervision of the risk management function (e.g. by conducting regular tests against relevant and known potential attacks to ensure that changes are correctly implemented and that possible vulnerabilities to observed security threats are identified).
- The GA has a requirement that CPS service providers implement IT environment segregation (e.g. of the development, test and production environments). To do so, the CPS service providers may consider the following (non-exhaustive) list of points:
  - rules for the transfer of software from development to operational status should be defined and documented;
  - software under development, software being tested and operational code should be isolated in different IT environments to ensure adequate segregation;
  - only executable code should be stored in the production environment; compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;
  - the test system environment should emulate the (live) operational system environment as closely as possible;
  - users should use different user profiles for operational and test systems, and menus should display appropriate system identification messages to mitigate the risk of error;
  - the transfer of sensitive payment data to the development and test environments should be avoided or, if necessary, allowed temporarily with specific control measures.

  Background documents and information:

  - *IT and data protection policies.*

In addition, the GA is encouraged to comply with the following best practice:

- The GA could provide security tools to protect customer interfaces against unlawful use or attacks (e.g. a secure interface provided by customised software running from a secure USB device, or dedicated security software for screening the customer's PC). The GA is invited to require CPS service providers to do the same.

3.1.4.3 STRONG CUSTOMER AUTHENTICATION, CRYPTOGRAPHY

Do the security features used for strong customer authentication follow publicly available and recognised standards? Where cryptographic security measures are used, are publicly known cryptographic algorithms with up-to-date, secure key lengths employed?

- The GA requires that the security features used for strong customer authentication follow publicly available and recognised standards:
  - the GA has defined a set of publicly known cryptographic algorithms (e.g. with recommended, state-of-the-art key lengths, algorithm specifications, information entropy[5]) to be used within the CPS;
  - for one-time passwords (OTPs), the password value is generated using secure devices and procedures based on publicly available and recognised standards; the procedure generates adequately complex passwords; the knowledge of a password value does not assist in deriving subsequent values.
- The GA requires that the confidentiality of the authentication value is protected from the moment it is generated to its verification by the authentication server.
- The GA periodically reassesses whether the algorithms and key lengths used are adequate to protect assets, including sensitive data and secrets. The GA accordingly updates its set of algorithms and key lengths to be used within the CPS. The GA has a procedure in place to ensure that all CPS service providers adapt accordingly.

  Background documents and information:

  - *list of recommended cryptographic algorithms;*
  - *password policy;*
  - *report on the use of cryptographic algorithms and passwords by service providers.*

3.1.4.4 COMPROMISED SECRETS

Is there a contingency plan in place outlining procedures to be followed in the event of secrets being compromised? Is this plan tested and reviewed on a regular basis?

- The GA has defined a contingency plan at the CPS level, outlining the procedures to be followed in the event of secrets being compromised.

5 In this context, the term "entropy" means a measure of the amount of uncertainty that an attacker faces in determining the value of a secret. This concept has been used in the context of information theory and cryptography as a measure of the difficulty in guessing or determining a password or a key.

- This contingency plan encompasses the identification of problems, containment, a fall-back solution and recovery procedures. The fall-back solution covers the risk of a single point of compromise. This plan also includes a clearly defined procedure for communicating with the CPS service providers. It is documented, tested and reviewed on a regular basis.

- The GA requires the CPS service providers to put in place such a contingency plan, together with a clearly defined procedure for communicating with the other CPS service providers and the GA.

  Background documents and information:

  – *procedures to be followed in the event of secrets being compromised;*

  – *contracts and specifically clauses on the obligation to deploy a contingency plan;*

  – *audits and issued recommendations.*

3.2 MANUFACTURE AND DISTRIBUTION OF CARDS

3.2.1 THE DESIGN AND MANUFACTURE OF PAYMENT CARDS AND OF ACCEPTING AND OTHER TECHNICAL DEVICES SHOULD ENSURE AN ADEQUATE DEGREE OF SECURITY IN LINE WITH THE SECURITY POLICIES OF THE CPS.

3.2.1.1 SECURITY REQUIREMENTS FOR CARDS AND DEVICES

Does the GA define security requirements, in line with the CPS's security policies, for cards, accepting devices and other technical devices which are of significant importance for the CPS? Does the GA check that these requirements are met within the CPS? Is it required that all cards issued be technically ready to be used with strong customer authentication?

- The GA has defined security requirements for cards, accepting devices and other technical devices which are of significant importance for the CPS, in line with the CPS's security policies.

- The GA requires the CPS service providers to comply with these requirements.

- The GA requires issuers to support strong customer authentication for all of their cards that can be used for internet payments. These cards that are used with strong customer authentication should be registered within issuers' IT systems. Exceptions must be based on risk analyses and subject to proper monitoring.

- The GA assesses, in line with the CPS's security policies, the need for an approval process for manufacturers of cards and technical devices, for example regarding the development process, a secure production environment and quality assurance measures.

  Background documents and information:

  – *CPS's security requirements for cards, accepting devices and other technical devices;*

  – *information on the process for assessing the implementation of the CPS's security requirements;*

– *list of the relevant controls performed (including external audits) and recommendations issued over the last two years;*

– *documentation on the approval of manufacturers of cards, accepting devices and other technical devices.*

3.2.1.2 EVALUATION OF DEVICES BY THIRD PARTIES

Do competent third parties (independent of the GA) evaluate the electronic components (e.g. cards) and devices (e.g. accepting devices) given to customers, as well as authentication procedures?

- The GA has defined or requires PSPs to define a formal approval procedure for the use of electronic components (e.g. cards, tokens) and devices (e.g. accepting devices) given to customers and, in particular, for the strong customer authentication procedure as a whole. This includes an evaluation and certification process as well as regular re-evaluations.

- Independent (of the GA/PSP) and competent (from a knowledge and reputational point of view) third parties evaluate and certify that the level of security for these devices and authentication procedures is sound and that they are tamper resistant:

  – the devices have been certified based on acknowledged standards or methodologies by certification authorities or have been evaluated (e.g. in a security report) by laboratories, university experts or technical consultants;

  – the tamper resistance is verified based on penetration tests and vulnerability assessments.

  Background documents and information:

  – *CPS's approval procedure for electronic devices;*

  – *list of the devices given to customers to operate strong customer authentication;*

  – *third-party certification or evaluations of devices;*

  – *reports on the efficiency of these devices (e.g. including fraud rates).*

3.2.1.3 EVALUATION OF DEVICES APPROVED BY OTHER CPSS

Where components (e.g. cards or accepting devices) approved by other CPSs are used, is it ensured that such components meet the CPS's own technical security standards?

- The GA has a process in place to ensure that where components approved by other CPSs are used, they meet the CPS's own technical security standards.

- The GA requires all of the CPS service providers to comply with these requirements.

  Background documents and information:

  – *CPS's process for evaluting components approved by other CPSs.*

3.2.1.4 SEPARATION OF EMBEDDED APPLICATIONS IN A CPS COMPONENT

When several kinds of applications (e.g. e-ticketing, card payment applications) are embedded in a CPS component, is it ensured that these are strictly separated (in terms of both logical design and technical security features)?

- The GA has clearly specified in its security requirements for the CPS that CPS and non-CPS applications embedded in a CPS component (used by customers of the CPS) have to be strictly separated. This separation exists from a logical design and a technical security point of view (this excludes the PIN itself if the PIN can be chosen by the cardholder or if the same security requirements for the protection of the PIN apply also to the other application).

- The GA requires the relevant CPS service providers to comply with these requirements.

  Background documents and information:

  – *CPS's security requirements for applications embedded in a CPS component;*

  – *information on the process for assessing the implementation of the CPS's security requirements;*

  – *list of the relevant controls performed (including external audits) and recommendations issued over the last two years.*

3.2.2 EFFECTIVE AND SECURE PROCEDURES SHOULD BE IN PLACE FOR THE INITIALISATION, PERSONALISATION AND DELIVERY OF BOTH CARDS TO HOLDERS AND ACCEPTING DEVICES TO ACCEPTORS, AND FOR THE GENERATION AND DELIVERY OF SECRETS (E.G. PIN).

3.2.2.1 INITIALISATION, PERSONALISATION AND DELIVERY OF CARDS

Is it ensured that effective and secure procedures and controls are in place regarding the personalisation and encoding of blank cards, the destruction of faulty cards prior to delivery to cardholders and the delivery of such cards? Are similar procedures and controls in place for other technical devices for the cardholders?

- The GA has defined an effective and secure process which includes secure procedures and controls regarding the personalisation and encoding of blank cards, the destruction of faulty cards before they are delivered to the cardholders and the delivery of such cards.

- The GA has defined and implemented similar procedures and controls (e.g. secure provisioning and deactivation mechanisms for payment applications on mobile devices) for other technical devices for the cardholders.

- The GA requires the relevant CPS service providers to comply with these requirements.

  Background documents and information:

  – *CPS's procedures and controls regarding the creation and delivery of cards and other technical devices to cardholders;*

– *information on the process for assessing the implementation of the CPS's procedures and controls;*

– *list of the relevant controls performed (including external audits) and recommendations issued over the last two years.*

3.2.2.2 PRODUCTION, DELIVERY AND INSTALLATION OF ACCEPTING DEVICES

Is it ensured that effective and secure procedures and controls are in place as regards the production, delivery and installation of accepting devices for acceptors?

- The GA has defined effective and secure procedures and controls as regards the production, delivery and installation of accepting devices for acceptors, including final acceptance procedures.

- The GA requires the relevant CPS service providers to comply with these requirements.

  Background documents and information:

  – *CPS's procedures and controls regarding the production, delivery and installation of accepting devices for acceptors;*

  – *information on the process for assessing the implementation of the CPS's procedures and controls;*

  – *list of the relevant controls performed (including external audits) and recommendations issued over the last two years.*

3.2.2.3 ROLLOUT, ENROLMENT FOR AND PROVISION OF AUTHENTICATION TOOLS AND/OR SOFTWARE DELIVERED TO THE CUSTOMER

Is it ensured that customer enrolment for and the initial provision of the authentication tools required to use the payment service (including internet payment services) and/or the delivery of payment-related software to customers is carried out in a secure manner?

- The GA requires that the enrolment for and the initial provision of the authentication tools required to use the payment service and/or the delivery of payment-related software to customers be carried out in a secure manner. More specifically, the GA requires that PSPs:

  – implement a procedure ensuring that the enrolment for and provision of authentication tools and/or payment-related software delivered to the customer takes place in a safe and trusted environment;

  – take into account possible risks related to the provided authentication tools and/or software delivered to the customer arising from the devices that are not under the PSP's control;

  – have effective and secure procedures in place for the delivery of personalised security credentials (e.g. separate delivery of devices and credentials, separate delivery channels);

  – have effective and secure procedures in place for the delivery of personalised payment-related software and of all payment-related personalised devices;

– ensure that software delivered via the internet is digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with;

– have a procedure in place to monitor the number of incidents related to the provision of authentication tools and the delivery of payment-related software.

Background documents and information:

– *procedures for the provision of authentication tools and personalised payment-related software to users.*

3.2.2.4 SECRETS AND AUTHENTICATION DEVICES

Does the CPS define procedures for the secure management (including delivery) of secrets (e.g. PINs, cryptographic keys, passwords), cardholder data, cards and accepting devices, as well as security requirements for authentication procedures and related devices (e.g. tokens, cryptographic devices)? Is compliance with these procedures checked on a regular basis?

- The GA has defined secure policies and procedures for managing secrets, cardholder data and authentication tools within the CPS and requires all CPS service providers to both comply with these requirements and ensure that their customers that are card acceptors do so as well. These policies and procedures cover PIN management and the whole life-cycle of cryptographic keys (e.g. generation, distribution, loading, storage, usage, backup/recovery, destruction and compromise, and password management).

- The GA requires that, where the activation of strong authentication during online shopping is offered, this activation is done by re-directing the customer to a safe and trusted environment.

- The GA requires all CPS service providers to comply with these requirements.

Background documents and information:

– *procedures for managing secrets, cardholder data, authentication means, cards and accepting devices;*

– *contracts and in particular clauses on secrets and authentication devices;*

– *audits and issued recommendations.*

3.2.2.5 AUTHENTICATION PROCEDURE

Does the CPS require issuers and acquirers to have a strong customer authentication procedure?

- The GA requires PSPs to have a strong customer authentication procedure ensuring that:

– two or more elements from at least two of the defined categories are used to prove the authenticity of the user[6];

6 Knowledge and ownership is allowed; ownership and ownership is not allowed.

- the security features of the solution are properly defined and implemented (e.g. algorithm specifications, key length, information entropy) and, in particular, that the OTP values are generated using secure devices and procedures based on publicly available and recognised standards, the resulting passwords are sufficiently complex and subsequent values cannot be derived from the knowledge of one password;

- the measures to mitigate risks (e.g. of malware infection or hacking attacks) related to the use of multi-purpose devices (e.g. mobile phones or tablets) are applied when multi-purpose devices are used as the ownership element (e.g. to receive or generate an OTP or initiate a drop call mechanism). Such measures could follow publicly available and recognised standards or could require that the payment itself is initiated via a separate/independent channel;

- the secrets used for the knowledge element are based on an appropriate and enforced password policy (information entropy, complexity, length, expiration time, number of characters that cannot be repeated, not guessable) or, if a non-password-based procedure is adopted, the likelihood of a false positive is comparable to or less than that for a (sound) password;

- the procedure and the chosen elements are designed in such a way as to ensure independence (e.g. in terms of the technology used, algorithms and parameters) so that the breach of one authentication element leaves the protection offered by the other elements unaffected (e.g. in the case of knowledge + ownership, the theft/misappropriation of one element leaves the effort necessary for the attacker to breach/bypass the other unchanged). Alternatively, in the case of co-dependence (e.g. where a PIN is used to initiate the generation of an OTP for a device) the risks are appropriately mitigated, taking into consideration: (a) specific security measures to avoid PIN guessing or retrieval from the device; (b) anti-cloning features of the device (e.g. smart card, token, SIM); and (c) particularly strong security features of the OTP generated (length, information entropy, random algorithms);

- the procedure is designed in such a way that the customer has to input all the credentials before receiving a positive or negative result; in cases of denied authentication, no information is given about which was the incorrect piece of data input (user ID, first element, second element, etc.);

- at least one of the selected elements falls into the inherence category or is non-reusable and non-replicable[7];

- the confidentiality of the authentication value is protected from the moment it is generated to its verification by the authentication server.

7 In this respect, authentication codes are non-replicable if the authenticator value (see below) is accepted only once by the authentication system, allowing the user to perform only a specific operation. It should also not be feasible to forge/clone an exploitable copy of the element (except for inherence), even if the element is available, nor to steal related confidential information (e.g. cryptographic keys, sensitive software or private keys for digital signatures) via the internet, including when not performing a payment-related transaction (e.g. via malware or advanced persistent threats). The authentication element (e.g. knowledge, ownership, inherence) produces a data string (e.g. password, OTP, biometric value) that is sent remotely to the authentication server during the payment initiation phase. This data string – the "authenticator value" – is transmitted via a protocol to the authentication server as proof that the user possesses and controls the "authentication element" and, consequently, as proof of the user's identity.

Background documents and information:

– *procedure for strong customer authentication.*

In addition, the GA is encouraged to comply with the following best practices:

- The GA could require PSPs to provide strong customer authentication solutions for which one (or more) of the selected elements entails transaction data signing specifying the amount and the cardholder, as well as the time stamp, and ensuring that the transaction cannot be altered. These solutions should be audited/reviewed, including for tamper resistance.

- The GA encourages PSPs, for convenience purposes, to offer the same strong customer authentication solution to all their customers and across all internet payment services. PSPs adopting such a practice define fall-back solutions covering the risk of a single point of compromise regarding the strong customer authentication tool.

3.2.2.6 DETECTION OF FRAUD DURING THE ACCESS PHASE

Is the CPS able to detect immediately the loss, theft or copying of card data or PINs during the personalisation and delivery process and to react immediately to prevent such cards from being used to conduct fraudulent transactions?

- The GA has a procedure in place to detect the fact that cards or PINs have been lost, stolen or copied.

- The GA has defined clear procedures to react immediately to fraudulent use in case of the loss, theft or copying of card data or PINs during the personalisation and delivery process. These procedures are regularly tested and updated if deemed relevant.

- The GA requires the relevant CPS service providers (including issuers and card manufacturers) to comply with all of the requirements specified above.

  Background documents and information:

  – *CPS's procedures to detect the compromise of cards or PINs during the personalisation and delivery process;*

  – *CPS's procedures to react to such situations;*

  – *information on the process for assessing the implementation of the above procedures;*

  – *list of the relevant controls performed (including external audits) and recommendations issued over the last two years.*

3.3 TRANSACTIONS

3.3.1 ADEQUATE SECURITY STANDARDS SHOULD BE IN FORCE FOR THE INITIATION OF TRANSACTIONS IN ACCORDANCE WITH CPS SECURITY POLICIES. CPS' COMPONENTS SHOULD BE PROTECTED FROM UNAUTHORISED ACTIVITY. THE CPS SHOULD HAVE THE CAPABILITY TO MITIGATE THE RISKS STEMMING FROM THE USE OF PAYMENT CARDS WITHOUT ONLINE AUTHORISATION OR WITH LESS SECURE AUTHENTICATION MEASURES (E.G. REMOTE PAYMENTS).

3.3.1.1 VALIDITY PERIODS

Are clear validity periods defined for payment cards, payment service sessions, authentication devices and secrets?

- The GA has defined and/or requires PSPs to define policies regarding appropriate validity periods for payment cards, authentication devices and secrets (including OTPs[8]) and a maximum number of failed log-in or authentication attempts (retry limits), after which access to the payment service is temporarily or permanently blocked, in line with the risk analysis. These policies take into account the lifetime of a key or a certificate and the associated renewal policy.

- The GA has defined or requires PSPs to define the maximum period of time after which inactive internet payment service sessions are automatically terminated (i.e. closing both application and network sessions) in line with the risk analysis.

- The GA requires all PSPs to comply with these policies.

  Background documents and information:

  – *general policies on expiry dates and secrets;*

  – *contractual clauses on expiry dates and secrets.*

  – *audits and issued recommendations.*

3.3.1.2 SCHEME SECURITY MEASURES

Are the CPS's security measures proportionate to the risks faced for the various types of transaction (e.g. off-line transactions, online transactions or card-not-present transactions, or checking the authenticity and validity of cards and accepting devices (if relevant) before the acceptance of a transaction)?

- The GA has defined security specifications for each transaction type used within the CPS, which are in line with the CPS's security policies. These specifications ensure for example that the authenticity and validity of cards and accepting devices (when relevant for a given transaction type) are checked before a transaction is accepted. These security specifications notably require that:

  – issuers support strong customer authentication for all transactions where the acquirer or wallet provider requests such authentication;

8 E.g. in some cases a validity period of less than 120 seconds might be appropriate for OTPs.

- acquirers or wallet providers can (e.g. for the first transaction or for card registration in a wallet) oblige the issuer to challenge the cardholder with strong customer authentication;

- PSPs carry out the initial registration for the implementation of virtual cards in a safe and trusted environment and perform strong customer authentication when generating virtual card data over the internet;

- acquirers implement strong customer authentication in their IT systems and protocols used to communicate with issuers. The implementation thereof should be audited/reviewed;

- acquirers require their e-merchants to support solutions allowing issuers to perform strong authentication of the cardholder for card-not-present transactions over the internet. Acquirers may allow e-merchants (via contracts) to use alternative authentication measures for pre-identified categories of low-risk transactions (e.g. based on a transaction risk analysis, or involving low-value payments) taking into account the nature of the products/services sold (e.g. physical vs. digital goods and services), the delivery channel, customer behaviour and the fraud monitoring capabilities of the e-merchants. Acquirers should maintain a list of their e-merchants having effective strong customer authentication solutions in place and be able to track transactions together with the method of authentication;

- wallet providers support strong customer authentication when customers log in to the wallet payment services or carry out card payments over the internet. Wallet providers may allow e-merchants (via contracts) to use alternative authentication measures for pre-identified categories of low-risk transactions (e.g. based on a transaction risk analysis, or involving low-value payments) taking into account the nature of the products/services sold (e.g. physical vs. digital goods and services), the delivery channel, customer behaviour and the fraud monitoring skills of the e-merchants.

- The GA requires aquirers to contractually require card acceptors to clearly separate payment-related processes from their online shops in order to make it easier for cardholders to identify when they are communicating with a PSP and not their payee (e.g. by re-directing the cardholder and opening a separate window so that the payment process is not shown as taking place within the online shop). Acquirers should raise the awareness of card acceptors about this issue and have a procedure to ensure compliance (e.g. fines, termination of contract).

  Background documents and information:

  - *security policy governing card transactions;*

  - *contractual clauses on card transactions and the separation of payment-related processes on card acceptors' websites;*

  - *audits and issued recommendations.*

3.3.1.3 DETECTION OF UNAUTHORISED ACTIVITIES

Has the GA defined a policy governing the detection of unauthorised activities?

- The GA has defined a requirement in its CPS security policy governing the detection of unauthorised activities.

- The GA's or the CPS service providers' applications are capable of providing audit trails including log-in, error and warning messages, as well as other information contained in log files (e.g. the transaction logs contain the correct transaction sequential numbers and timestamps). The timestamps included in log files and audit trails are accurate (e.g. by regularly synchronising servers with one or more trusted time sources such as a time server or GPS).

- The GA ensures or requires service providers to ensure that log files accurately trace parameterisation changes, accesses and attempts to access transaction data. This requirement includes the obligation to identify the originator of the unauthorised activity. The log files are tamper-proof and can only be accessed by authorised personnel or applications. They are stored for an adequate period, in line with local regulations.

- The GA regularly analyses or requires service providers to analyse log files and audit trails and take correctional and/or preventive measures.

- The GA ensures or requires service providers to ensure that their service incorporates security mechanisms for the detailed logging of transaction data.

- The GA requires all CPS service providers to report monitoring activities (e.g. using software tools and processes to evaluate log files, with periodical queries and analyses of logged transaction data for inconsistencies, signs of tampering and unauthorised access).

  Background documents and information:

  – *security policy governing the detection of fraud in relation to transaction data;*

  – *reports on unauthorised access to and attempts to access transaction data;*

  – *audits and issued recommendations.*

In addition, the GA is encouraged to comply with the following best practice:

- The GA could require acquirers to contractually require its customers who store payment information to have adequate processes in place to support traceability and report relevant issues to the PSP.

3.3.2 THE ACTIVITIES OF CARDHOLDERS AND CARD ACCEPTORS SHOULD BE PERMANENTLY MONITORED IN ORDER TO ENABLE A TIMELY REACTION TO FRAUD AND ANY RISKS POSED BY SUCH ACTIVITIES. APPROPRIATE MEASURES SHOULD BE IN PLACE TO LIMIT THE IMPACT OF FRAUD

3.3.2.1 FRAUD MONITORING

Has the CPS put in place a fraud monitoring framework, in line with and linked to the risk analysis?

- The GA has defined the various types of fraud within the CPS.

- The GA has defined procedures to collect fraud data (e.g. fraud detection and prevention solutions are in place to identify suspicious transactions before their processing) and monitors fraud within the CPS. These procedures are in line with and linked to the GA's risk analysis.

- The GA requires CPS service provider to adopt fraud detection and prevention solutions in line with and linked to their risk analyses and report to the GA fraud events with potential significant repercussions for the CPS.

- The GA has, in cooperation with acquirers, elaborated a harmonised definition of e-merchant categories which follows standards established for traditional/physical payments and requires acquirers to implement it accordingly in the authorisation message conveyed to the issuer.

- The GA requires issuers to be able to detect fraud and have fraud prevention solutions in place that use parameterised rules (e.g. black lists of compromised or stolen card data or data breaches, IP or IP range change during the internet session, potentially abnormal customer behaviour, atypical e-merchant categories for a specific customer, signs of malware), which are sufficiently defined and updated on a regular basis. The solutions in place are able to detect and give warning of suspicious transactions.

- The GA requires acquirers to have fraud detection solutions implemented in a way that allows the monitoring of cardholders' activities on the basis of transaction patterns (e.g. transaction amounts and numbers), e-merchant categories and geolocation.

- The GA requires PSPs to use an appropriate time frame for transaction screening procedures (and potential fraud evaluation) which ensures that the initiation and/or execution of the transaction are not unduly delayed (in line with the provisions of the PSD).

  Background documents and information:

  – *lists of identified types of suspicious transactions and fraud;*

  – *procedures in place to detect and report suspicious transactions and monitor fraud;*

  – *audits and issued recommendations.*

3.3.2.2 REACTION TO FRAUD

Is the CPS able to react in a timely manner in the event of fraud in order to limit its financial impact?

- The GA has conducted an analysis regarding the financial impact of fraud within the CPS.

- Based on this analysis, the GA has defined clear procedures and reaction times which are proportionate to the respective fraud events.

- The GA has defined a procedure to review the above analysis and corresponding reaction procedures.

- The GA requires all CPS service providers to comply with these procedures.

  Background documents and information:

  – *report on the financial impact of fraud within the CPS;*

– *list of procedures and reaction times in response to fraud events;*

– *scheme rules and contractual clauses on procedures followed in response to fraud;*

– *audits and issued recommendations.*

In addition, the GA is encouraged to comply with the following best practice:

- The GA could require issuers to implement alerts for customers, such as via phone calls or SMS, for suspicious or high-risk payment transactions based on their risk management policies. The procedure could set a default amount limit that triggers an alert, with the option to lower that limit. The alerts are secure, clear and in line with the issuers' risk management policies.

3.3.2.3 FRAUD IMPACT MITIGATION

Does the CPS define security measures to mitigate the impact of fraud in line with the security policy? Are security measures in place (e.g. card revocation, rapid change of secrets, transaction limits)?

- The GA has conducted an analysis of the impact of fraud and has defined adequate security policies and measures for fraud mitigation. These include the ability to suspend (temporarily or permanently) access to the payment service, a limited number of off-line transactions, procedures to disable the use of cards (including over the internet), procedures for changing secrets, a facility to manage transaction limits (e.g. the maximum amount for each individual payment or a cumulative amount over a certain period of time), a mechanism to prevent double log-in and cardholder verification methods. The GA requires that issuers have defined specific secure procedures to reactivate the use of cards.

- The GA requires issuers to:

  – prior to providing payment services to their customers, have defined limits (e.g. the maximum amount for each individual payment or a cumulative amount over a certain period of time, or an amount specific to card payments over the internet) that are proportionate to the risks involved in the services provided and have informed their customers accordingly;

  – have defined and documented procedures (technical or other) to ensure that blocked transactions are kept in that status for as short a time as possible;

  – allow their customers to disable the internet payment functionality of their cards.

  Background documents and information:

  – *security policies and fraud mitigation procedures;*

  – *scheme rules and contractual clauses on fraud mitigation;*

  – *audits and issued recommendations.*

In addition, the GA is encouraged to comply with the following best practices:

- The GA could require issuers to:

  – provide their customers with the facility to manage limits for the use of cards in a safe and trusted environment. The dedicated procedure has been clearly explained to customers (e.g. when changes of limits become effective);

  – enable their customers to specify, in a safe and trusted environment, general, personalised rules as parameters for their behaviour with regard to card payments (including over the internet) and related services (e.g. that they will initiate card payments in specific countries and that payments initiated from elsewhere should be blocked). These personalised rules and parameters have been clearly explained to customers and can be changed by customers in a secure and convenient manner;

  – when providing such services, keep track of the changes to the limits and personalised rules and make them available to their customers via the predefined communication channel (e.g. their online banking). Moreover, they should notify their customers of any changes made to the limits via an out-of-the-band channel (e.g. SMS alerts).

3.3.2.4 INCENTIVE MECHANISM FOR SECURITY IMPROVEMENTS AND ANTI-FRAUD TECHNOLOGIES

Are there any incentive mechanisms in place (e.g. liability shifts) to improve security and anti-fraud technologies?

- The GA has implemented a liability shift towards a PSP failing to support strong customer authentication for all card payments. The resulting liability regime is transparent, clear and enforceable, and includes a dispute resolution mechanism.

- The GA could define and promote additional incentive mechanisms aimed at improving security and anti-fraud technologies within the CPS. These mechanisms could be pricing incentives (e.g. interchange fees) which encourage issuers/acquirers to invest in security.

  Background documents and information:

  – *contractual clauses on liability shifts and security improvements;*

  – *audits and issued recommendations.*

3.3.3 APPROPRIATE ARRANGEMENTS SHOULD BE MADE TO ENSURE THAT CARD TRANSACTIONS CAN BE PROCESSED EVEN AT PEAK TIMES AND ON PEAK DAYS.

3.3.3.1 CAPACITY MONITORING

Is effective monitoring of the overall traffic flow, capacity and performance of sensitive operations related to card transaction processing (e.g. the authorisation process) in place?

- The GA has identified and classified all sensitive operations related to card transaction processing (e.g. the authorisation process).

- The GA has put in place procedures to monitor the traffic flows, capacity and performance of those operations. The GA requires CPS service providers to act accordingly.

- The GA has defined a process to verify the efficiency of the monitoring procedure.

  Background documents and information:

  – *list of sensitive operations;*

  – *list of procedures to monitor traffic flows, capacity and performance;*

  – *audits and issued recommendations.*

3.3.3.2 CAPACITY PLANNING

Is processing capacity enhanced in time to avoid systemic disruptions to card transactions and possible bottlenecks, especially at peak times and on peak days?

- The GA has defined or requires CPS service providers to define a procedure to periodically assess the CPS's processing capacity and, if relevant, to analyse the causes of potential deviations and to initiate remedial actions. The goal of this procedure is to avoid systemic disruptions to card transactions, as well as other possible bottlenecks, taking into account peak times and peak days in the system.

  Background documents and information:

  – *list of procedures relating to processing capacity.*

3.3.4 SUFFICIENT EVIDENCE SHOULD BE PROVIDED TO ENABLE A TRANSPARENT AND EASY CLARIFICATION OF DISPUTES BETWEEN ACTORS

3.3.4.1 DISPUTE RESOLUTION EVIDENCE

Is sufficient evidence provided to enable disputes to be resolved and to demonstrate the validity of transactions (identification of payer and payee, transaction amount, etc.)?

- The GA has defined the evidence that should be provided to demonstrate the validity of transactions and to enable disputes to be resolved.

- The GA requires CPS service providers to implement procedures to collect this evidence and provide it at least upon request.

  Background documents and information:

  – *list of the pieces of evidence to be provided to demonstrate the validity of transactions.*

3.4 CLEARING AND SETTLEMENT

3.4.1 CLEARING AND SETTLEMENT ARRANGEMENTS SHOULD ENSURE AN ADEQUATE DEGREE OF SECURITY, OPERATIONAL RELIABILITY AND AVAILABILITY, TAKING INTO ACCOUNT THE SETTLEMENT DEADLINES SPECIFIED BY THE CPS

3.4.1.1 TECHNICAL AND ORGANISATIONAL SECURITY REQUIREMENTS

Are appropriate technical and organisational security requirements defined for clearing and settlement (including requirements governing processing capacity and availability), taking into account settlement deadlines specified by the CPS?

- If the GA has defined settlement deadlines, these deadlines are in line with the service level which is transparent to all actors.

- The GA has defined technical and organisational security requirements for clearing and settlement[9], taking into account specified settlement deadlines. These requirements include measures relating to capacity, availability, confidentiality, auditability, integrity and authenticity.

- The GA requires CPS service providers to define adequate security requirements for clearing and settlement arrangements, taking into account the settlement deadlines specified by the GA.

  Background documents and information:

  – *list of security requirements and deadlines for clearing and settlement;*

  – *contractual clauses on security requirements and deadlines for clearing and settlement;*

  – *audits and issued recommendations.*

3.4.1.2 FULFILMENT OF REQUIREMENTS

Is the fulfilment of these requirements assessed by the GA on a regular/event-driven basis?

(Clearing and settlement arrangements and systems which are already covered by oversight are excluded.)

- The GA has a process to assess on a regular/event-driven basis (e.g. through on-site inspections) clearing and settlement arrangements regarding the fulfilment of the CPS's requirements.

- The GA could consider, for instance, assessments or activities carried out as a part of banking supervision.

  Background documents and information:

  – *audits and issued recommendations.*

9 The monitoring of the operational reliability of clearing and settlement agents is covered by assessment questions 5.1.5 and 5.1.6.

3.4.1.3 UNAVAILABILITY AND RELIABILITY PROBLEMS

Are risks relating to unavailability and operational reliability problems within clearing and settlement processes mitigated, taking into account the settlement deadlines specified by the CPS?

(Clearing and settlement arrangements and systems which are already covered by oversight are excluded.)

- If the GA has not defined settlement deadlines, there is no specific need for risk mitigation. If the GA has defined settlement deadlines, the GA has a process in place to ensure that identified risks to availability or operational reliability within clearing and settlement arrangements are mitigated, avoiding the existence of single points of failure (e.g. alternative clearing and settlement arrangements are in place, appropriate technical redundancy of clearing and settlement arrangements is provided).

  Background documents and information:

  – *policy on identifying risks to availability and operational reliability;*

  – *audits and issued recommendations.*

3.5 BUSINESS CONTINUITY

3.5.1 BUSINESS IMPACT ANALYSES SHOULD CLEARLY IDENTIFY THE COMPONENTS THAT ARE CRUCIAL TO THE SMOOTH FUNCTIONING OF THE CPS. EFFECTIVE AND COMPREHENSIVE CONTINGENCY PLANS SHOULD BE IN PLACE IN THE EVENT OF A DISASTER OR ANY INCIDENT THAT JEOPARDISES CPS AVAILABILITY. THE ADEQUACY AND EFFICIENCY OF SUCH PLANS SHOULD BE TESTED AND REVIEWED REGULARLY

3.5.1.1 BUSINESS CONTINUITY PLANS

Has the CPS identified components and processes which are essential to its smooth functioning and defined business continuity plans, including contingency processing arrangements, in line with the security policy and the agreed service level?

- The GA has identified all components and processes which are essential to the smooth functioning of the CPS (e.g. online authorisation and processing of card transactions on the acquiring and issuing side).

- The GA has defined a service level necessary for the smooth functioning of the CPS.

- The GA has defined business continuity plans for components which are essential to the smooth functioning of the CPS, including contingency processing arrangements (e.g. mechanisms in order to solve major hardware and software problems) in line with the security policy and the agreed service level(s).

- The business continuity plans define a business continuity strategy, identify critical functions and formulate resumption and recovery objectives. The plans consider issues related to scenarios, the secondary site(s), staff, and dependence on third parties, service providers and other actors. Crisis management and crisis communication management are an essential part of the plans.

- The GA requires CPS service providers to define appropriate business continuity plans for components which are essential to the smooth functioning of the CPS, including contingency processing arrangements (e.g. mechanisms to solve major hardware and software incidents) in line with the security policy of the CPS and the agreed CPS service level(s).

  Background documents and information:

  – *lists of the components and processes essential to the smooth functioning of the CPS;*

  – *CPS's business continuity plan;*

  – *sufficient information about issues related to scenarios, the secondary site(s), staff, and dependence on third parties, service providers and other actors;*

  – *CPS's crisis management and crisis communication management arrangements.*

3.5.1.2 BUSINESS CONTINUITY TESTING

Are the effectiveness and adequacy of the business continuity plans tested and reviewed on a regular/event-driven basis?

- The GA has a process in place to ensure that the effectiveness and adequacy of business continuity plans are reviewed on a regular/event-driven basis (e.g. the GA could consider assessments or activities carried out as part of banking supervision). These reviews include the testing, updating and communication of business continuity plans.

- The GA requires the CPS service providers to arrange similar reviews and to update their processes.

  Background documents and information:

  – *audits and issued recommendations.*

3.6 OUTSOURCING

3.6.1 SPECIFIC RISKS RESULTING FROM OUTSOURCING SHOULD BE MANAGED EXPLICITLY AND APPROPRIATELY THROUGH COMPREHENSIVE AND APPROPRIATE CONTRACTUAL PROVISIONS. THESE PROVISIONS SHOULD COVER ALL RELEVANT ISSUES FOR WHICH THE ACTOR WHO OUTSOURCES ACTIVITIES WITHIN THE CPS IS RESPONSIBLE

3.6.1.1 OUTSOURCING RISK ANALYSIS

Does the CPS analyse specific risks relating to outsourcing and their impact?

The GA could, for instance, consider assessments/activities carried out as part of banking supervision.

- The GA has identified its sensitive activities relating to outsourcing. This information is kept up to date.

- The GA requires CPS service providers to do the same.

- The GA analyses risks and impacts for the CPS relating to these activities (e.g. there is sufficient control regarding whether service levels are always ensured or mitigation procedures are in place where this is not ensured). The analysis takes into account risks stemming from additional interfaces with outsourcing partners, unbalanced dependencies, loss of know-how and competences, security and data privacy aspects, the concentration ratio of outsourcing partners and the possible implications that this could have for the service levels of the CPS.

- The GA requires CPS service providers to analyse the specific risks related to these outsourcing activities and their impact.

  Background documents and information:

  – *list of specific risks related to outsourcing activities and their impact;*

  – *information about the outsourcing to third parties directly handled by the GA.*

3.6.1.2 CONTRACTUAL PROVISIONS

Do the contractual provisions cover all relevant issues for which the actor outsourcing activities within the CPS is responsible?

The GA could, for instance, consider assessments/activities carried out as part of banking supervision.

- The contracts with the providers of outsourced services (e.g. communication network facilities) include at least the following provisions:

  – requiring those service providers to conduct a risk assessment, take appropriate actions and report the results of both to the outsourcer;

  – enabling the outsourcer to check that the external provider meets these requirements.

- The GA has sought legal advice (e.g. from internal/external lawyers) about the coverage of all of its outsourcing activities (e.g. that might exacerbate operational risk) in its contractual provisions.

- The GA requires CPS service providers to also obtain legal advice about the coverage of all outsourcing activities in their contractual provisions.

  Background documents and information:

  – *legal advice received on the coverage of outsourcing activities of the GA in the contractual provisions;*

  – *legal issues with regard to specific contractual provisions related to outsourcing activities of the GA envisaged under the different jurisdictions where the CPS operates;*

  – *contractual clauses on outsourcing.*

3.6.1.3 SERVICE LEVEL AGREEMENT AND LIABILITIES

Does the CPS have contractual provisions covering its outsourcing partners to ensure continuity and the maintenance of expected service levels and to delineate the liabilities and responsibilities of each individual party?

The GA could, for instance, consider assessments/activities carried out as part of banking supervision.

- The GA has set a rule prohibiting outsourcing partners from working for/within the scheme without having signed a contract.

- The GA has a process in place to ensure that contracts with outsourcing partners contain clear descriptions of the expected service levels, including issues related to business continuity and risk management, and clearly outline the liabilities and responsibilities of the contractual parties (also in the event of an emergency).

- The GA requires CPS service providers to do the same.

  Background documents and information:

  – *list of outsourcing partners;*

  – *contracts signed with outsourcing partners;*

  – *audits and issued recommendations.*

3.6.2 OUTSOURCING PARTNERS SHOULD BE APPROPRIATELY MANAGED AND MONITORED. ACTORS WHO OUTSOURCE ACTIVITIES SHOULD BE ABLE TO PROVIDE EVIDENCE THAT THEIR OUTSOURCING PARTNERS COMPLY WITH THE STANDARDS FOR WHICH THE ACTOR ITSELF IS RESPONSIBLE WITHIN THE CPS

3.6.2.1 MONITORING

Does the GA regularly monitor the security, availability and performance of the services delivered by the outsourcing partners?

The GA could, for instance, consider assessments/activities carried out as part of banking supervision.

- The GA has a process in place to monitor the security, availability and performance of outsourcing partners in accordance with the respective contracts.

- The GA requires CPS service providers to have the same process.

  Background documents and information:

  – *report on outsourced activities.*

3.6.2.2 COMPLIANCE

Is it ensured that, in the event of an outsourcing partner not complying with the standards that it is required to meet within the CPS, such compliance is re-established immediately?

- The GA has a process in place to immediately re-establish compliance with the standards to be met by an outsourcing partner, in line with the respective contract.
- The GA requires CPS service providers to have the same process.

  Background documents and information:

  – *process in place to re-establish compliance with the standards governing outsourcing.*

4 THE CARD PAYMENT SCHEME SHOULD HAVE EFFECTIVE, ACCOUNTABLE AND TRANSPARENT GOVERNANCE ARRANGEMENTS

4.1 EFFECTIVE, EFFICIENT AND TRANSPARENT PROCESSES SHOULD BE DEFINED AND IMPLEMENTED WHEN

– MAKING DECISIONS ABOUT BUSINESS OBJECTIVES AND POLICIES, INCLUDING ACCESS POLICIES ON ISSUERS AND ACQUIRERS

4.1.1 ROLES AND RESPONSIBILITIES IN DECISION-MAKING

Are the roles and responsibilities of all actors involved in the decision-making processes clearly defined, disclosed (on a need-to-know basis) and enforced?

- The GA has identified roles and responsibilities of CPS actors involved in the decision-making process (e.g. ownership, management, decision-making bodies).
- The GA has a process in place to update these roles and responsibilities on a regular/event-driven basis.
- The GA discloses information on these roles and responsibilities to all actors and potential actors on a need-to-know basis (e.g. the GA has defined a classification procedure based on sensitivity).
- The GA requires all actors involved to follow roles and lines of responsibility within the decision-making process.
- If the functions of the GA are assumed by several entities, those entities:
  - adopt a clear and effective control of the scheme;
  - clearly define the level of decisional autonomy of each entity as well as issues which have to be decided by all GA entities together.

  Background documents and information:

  - *list of actors involved in the decision-making process and their specific roles and responsibilities;*
  - *policy governing the decision-making process.*

4.1.2 RULES FOR DECISION-MAKING

Are the rules for the decision-making process clearly defined and transparent given the size, complexity, structure, economic significance and risk profile of the CPS?

- The GA has defined the CPS's rules for the decision-making process (e.g. composition/competences/voting rights of the decision-making bodies, involvement of actors, etc.).
- These rules are in line with the CPS's size (taking into account all functions and the number of actors), its complexity (e.g. types of actors, licensees, etc.), its structure (e.g. three-party/four-party, Europe-wide/worldwide, type of company and law applicable, etc.), its economic significance

(e.g. market share, basic accounting data, etc.), its risk profile (e.g. identification of risks, definition of risk appetite, mitigation of the risk level, etc.).

- The GA has a procedure in place to regularly reassess the adequacy of the CPS's rules in place against the different criteria mentioned.

- The GA discloses information on these roles and responsibilities to all actors and potential actors on a need-to-know basis (e.g. the GA has defined a classification procedure based on sensitivity).

  Background documents and information:

  – *rules and procedures for the CPS's decision-making process.*

4.1.3 ACCESS POLICIES

Are access policies for CPS service providers determined on an objective, fair and transparent basis? Where applicants are rejected, is this communicated within an appropriate period of time, with reasons given for the rejection? Are the rules for the termination of and exit from a CPS clearly defined and transparent to the relevant service providers?

- The GA has set rules for access policies (e.g. relating to entry fees, financial stability, technical capacity, legal conformity) on the basis of fair, non-discriminatory criteria. Restrictive access criteria need to be justified on the basis of efficiency and/or security considerations for the scheme itself (justification on the basis of the PSD is possible as well).

- The GA communicates to actors and potential actors its access policies, including restrictive access criteria (e.g. risk ratings, security requirements, other indicators).

- If applicants are rejected, this is communicated to them within an appropriate period of time, with detailed information on the reasons for rejection.

- The GA has set explicit and clear rules for the termination of and exit from a CPS.

  Background documents and information:

  – *CPS access policy;*

  – *rules for the termination of and exit from the CPS.*

4.1.4 CONSULTATION OF ACTORS

Are relevant CPS actors consulted during the CPS's decision-making process as regards major changes (e.g. concerning technology, liability shifts, company structures, multilateral interchange fees or rules)?

- The GA has defined a classification for changes based on their significance.

- For major changes (e.g. in technology, liability, company structure, multilateral interchange fees, rules, etc.), all the relevant CPS actors are consulted (e.g. in a user group) as part of a structured procedure.

- These consultations are documented and the results are communicated to the decision-making bodies.

  Background documents and information:

  – *CPS classification for changes based on their significance;*

  – *procedure governing the consultation of all actors on major changes.*

– **REVIEWING THE PERFORMANCE, USABILITY AND CONVENIENCE OF THE CARD PAYMENT SCHEME; AND**

4.1.5 REVIEW OF SERVICES

Are there adequate processes in place to analyse the performance, usability and convenience of the services offered to customers by the CPS?

- The GA has a process in place to review the performance of the services offered to customers against its business objectives and policies.

- The GA has a process in place to regularly evaluate customer satisfaction, including security-related customer complaints. The findings are reported to the Board and the lessons learned from the relevant incidents/complaints are taken into account in the security policies and the incident management of the GA.

- The GA has adequate policies and processes in place to enhance and ensure sufficient usability, performance and convenience of the services offered to customers by the CPS service providers.

- The GA requires PSPs to do the same.

  Background documents and information:

  – *CPS's customer satisfaction analysis/report;*

  – *CPS's performance, usability and convenience review.*

– **IDENTIFYING, MITIGATING AND REPORTING SIGNIFICANT RISKS TO ITS BUSINESS**

4.1.6 RISK MANAGEMENT PROCESS

Does the GA apply a risk management process to identify and mitigate all related risks (in particular legal, operational, financial and reputational risks, as well as general management-related risks)?

- The GA has defined a risk management process that ensures the continuous monitoring of risk exposures and immediate reporting to the GA.

- The risk management process is reviewed on a regular/event-driven basis, taking into account internal and external changes.

- Where CPS service providers are involved, the GA requires them to act in the same manner.

Background documents and information:

– *risk management process;*

– *CPS's risk management framework (rules, policies, procedures and measures);*

– *audits and issued recommendations.*

4.2 THERE SHOULD EXIST AN EFFECTIVE INTERNAL CONTROL FRAMEWORK, INCLUDING AN ADEQUATE AND INDEPENDENT AUDIT FUNCTION

4.2.1 INTERNAL CONTROL FRAMEWORK

Has the GA adopted an internal control framework for the CPS? Does the GA monitor the compliance with the CPS's rules and procedures by issuers, acquirers and other service providers?

- The GA has an internal control framework in place for the CPS that includes an audit function with adequate resources (staff, technology, etc.). The internal control framework covers, for example, the definition of roles, responsibilities, competences, limits and accounting.

- If the GA requires changes as a result of audit findings within the internal control framework, there is a process in place to ensure that those changes are implemented in all the internal rules.

- The GA ensures that all relevant actors are consulted regarding any major changes and that an appropriate time frame is foreseen for the implementation thereof.

Background documents and information:

– *description of the CPS's internal control framework;*

– *list of staff in charge of the audit function;*

– *audits and issued recommendations.*

4.2.2 INDEPENDENT CONTROL FUNCTIONS

Does the GA ensure the independence of the CPS's control functions (e.g. appropriate level of reporting, internal/external audit)?

- The GA has a procedure in place to ensure that the GA's control functions (including audit functions) have appropriate competences and that they can report directly to the appropriate decision-making body of the GA.

- The GA's control functions (including audit functions) have appropriate independence (e.g. from the management, the owner, members, operational functions, etc.) to avoid any conflict of interest with the other functions (i.e. the trusted experts are not involved in any way in the development, implementation or operational management of the payment services).

- The GA requires CPS service providers to have similar procedures in place.

Background documents and information:

- *rules and policies governing the CPS's audit function;*
- *CPS's internal control and audit programme.*

4.2.3 EFFECTIVE CONTROL FUNCTION

Is the control framework effective in preventing and detecting irregular events?

- The GA has a procedure in place to review – on a regular/event-driven basis (e.g. major changes) – the effectiveness of the control framework, including whether it is able to prevent and detect serious and irregular events. The GA takes into consideration the risks involved to determine the frequency and focus of audits.

- The GA has a procedure in place for immediate reporting when serious deviations from the CPS's rules or other irregular events are detected (where external auditors are used, this is ensured in the contractual provisions). The GA requires CPS service providers to comply with these procedures. The GA can ask for audit reports from CPS service providers on issues pertaining to contracts, the manufacturing and distribution of cards, accepting and other technical devices, scheme security policies and measures, capacity monitoring and planning, business continuity, outsourcing and the independence of the control function. It has a procedure to enforce compliance with scheme rules and contracts and, when necessary, exclude the actor from the scheme.

- The GA requires acquirers to carry out regular checks on those card acceptors that handle sensitive payment data (e.g. audits or by requiring the e-merchant to provide audit reports). In the case of non-compliance by the card acceptor, the acquirer can take measures to enforce the contractual obligation or terminate the contract.

  Background documents and information:

  - *procedure for reviewing the effectiveness of the control framework;*
  - *procedure for reporting deviations from the CPS's rules;*
  - *relevant clauses in contracts with PSPs;*
  - *audits and issued recommendations.*

5 THE CARD PAYMENT SCHEME SHOULD MANAGE AND CONTAIN FINANCIAL RISKS IN RELATION TO THE CLEARING AND SETTLEMENT PROCESS

5.1 THE CARD PAYMENT SCHEME SHOULD IDENTIFY THE FINANCIAL RISKS INVOLVED IN CLEARING AND SETTLEMENT ARRANGEMENTS AND SHOULD DEFINE APPROPRIATE MEASURES TO ADDRESS THESE RISKS.

5.1.1 CLEARING ARRANGEMENTS

Does the GA have a complete overview of all existing arrangements for clearing, including major in-house clearing arrangements?

- The GA has a complete overview of all existing clearing arrangements. This also includes information on major in-house clearing activities within the scheme.

  Background documents and information:

  – *list of all clearing arrangements used in the CPS;*

  – *documentation and contracts regarding clearing arrangements;*

  – *information about how clearing takes place within the scheme and which percentage relates to in-house transactions.*

5.1.2 SETTLEMENT ARRANGEMENTS

Does the GA have a complete overview of all existing arrangements for settlement, including in-house settlement?

- The GA has a complete overview of all relevant existing arrangements for settlement. This also includes information on major in-house settlement within the scheme and correspondent banking.

  Background documents and information:

  – *list of settlement arrangements used in the CPS;*

  – *documentation and contracts regarding settlement arrangements;*

  – *information about how settlement takes place within the scheme and which percentage relates to in-house transactions and correspondent banking.*

5.1.3 FINANCIAL RISKS ARISING FROM CLEARING ARRANGEMENTS AND CLEARING AGENTS

Does the GA evaluate the financial risks arising from the different clearing arrangements and clearing agents used within the CPS? Does the GA mitigate financial risks which exceed its risk appetite? Are remaining financial risks accepted by the GA?

(Clearing arrangements and systems which are already covered by oversight are excluded.)

- The GA evaluates the financial risks arising from the different clearing arrangements used within the scheme that might result in a financial risk for the CPS. This should include financial

risks related to the default, insolvency or operational breakdown of a clearing agent and should take into consideration whether or not these clearing agents are engaged in other activites which might have an impact on the functioning of the clearing activity.

- The GA has defined a procedure for evaluating financial risks when selecting clearing agents or there are minimum requirements for PSPs participating in the scheme to select clearing agents. The risk profiles of clearing agents are taken into account.

- The GA has determined its risk appetite for clearing within the CPS and has formally accepted the remaining financial risks.

- The GA has a procedure to manage and contain the financial risks that exceed its risk appetite. It has appropriate measures in place for clearing arrangements which are a service of the GA or are offered by a company owned by the GA and requires the clearing agent, via a contract or rules, to have in place risk mitigation procedures to address such risks appropriately.

  Background documents and information:

  – *evaluation of the financial risks arising from clearing arrangements that might result in a financial risk for the CPS;*

  – *selection procedure and criteria for clearing agents;*

  – *CPS's financial risk analysis and management report;*

  – *CPS's financial risk mitigation policies and measures;*

  – *CPS's risk appetite and information on any residual financial risks formally accepted by the GA.*

5.1.4 FINANCIAL RISKS ARISING FROM SETTLEMENT ARRANGEMENTS AND SETTLEMENT AGENTS

Does the GA evaluate the financial risks arising from the different settlement arrangements and settlement agents used within the scheme? Does the GA mitigate financial risks exceeding its risk appetite? Are remaining financial risks accepted by the GA?

(Settlement arrangements and systems which are already covered by oversight are excluded.)

- The GA evaluates the financial risks arising from the different settlement arrangements used within the scheme. This should include financial risks related to the default, insolvency or operational breakdown of the settlement agent and should take into consideration whether or not these settlement agents are engaged in other activities which might have an impact on the functioning of the settlement activity.

- The GA has defined a procedure for evaluating financial risks when selecting settlement agents or there are minimum requirements for PSPs participating in the scheme to select settlement agents. The risk profiles of settlement agents are taken into account.

- The GA has determined its risk appetite for settlement within the CPS and has formally accepted the residual financial risks.

- The GA has a procedure to manage and contain the financial risks that exceed its risk appetite. It has appropriate measures in place to address credit and liquidity risks for settlement arrangements which are a service of the GA or are offered by a company owned by the GA and requires the clearing agent, via a contract or rules, to have in place risk mitigation procedures to address such risks appropriately.

  Background documents and information:

  – *evaluation of the financial risks arising from settlement arrangements that might result in a financial risk for the CPS;*

  – *selection procedure and criteria for settlement agents;*

  – *CPS's financial risk analysis and management report;*

  – *CPS's financial risk mitigation policies and measures;*

  – *CPS's settlement risk appetite and information on any residual financial risks formally accepted by the GA.*

5.1.5 MONITORING OF CLEARING AGENTS

Does the GA monitor financial, operational and security risks of clearing agents in line with its overall risk appetite?

(Clearing arrangements and systems which are already covered by oversight are excluded.)

- If clearing agents engage in activities that represent financial risks, the GA monitors the creditworthiness of clearing agents and takes action based on the results of this monitoring.

- The GA monitors the operational reliability (including security risks) of clearing agents and takes action based on the results of this monitoring.

  Background documents and information:

  – *analysis of the financial, operational and security risks of clearing agents;*

  – *scheme rules and proof of the monitoring.*

5.1.6 MONITORING OF SETTLEMENT AGENTS

Does the GA monitor financial, operational and security risks of settlement agents in line with its overall risk appetite?

Settlement arrangements and systems which are already covered by oversight are excluded.

- The GA monitors or requires scheme participants to monitor the creditworthiness of settlement agents and takes action based on the results of this monitoring.

- The GA monitors or requires scheme participants to monitor the operational reliability (including security risks) of settlement agents and takes action based on the results of this monitoring.

  Background documents and information:

  – *procedure for monitoring settlement agents.*

5.2 CLEARING AND/OR SETTLEMENT PROVIDERS

THE CARD PAYMENT SCHEME SHOULD ENSURE THAT ALL SELECTED CLEARING AND SETTLEMENT PROVIDERS ARE OF SUFFICIENT CREDITWORTHINESS, OPERATIONAL RELIABILITY AND SECURITY FOR THEIR PURPOSES.

5.2.1 SELECTION PROCEDURE

In choosing their clearing and/or settlement providers, do CPS actors consider financial, operational and security risks in order to choose a provider in line with their overall risk appetite?

- The GA has a procedure to identify the financial, operational and security risks when choosing its clearing and settlement providers, has evaluated these risks, recognising any trade-offs between them that may be necessary, and has chosen a provider in line with the CPS's overall risk appetite.

- The GA requires other CPS actors to do the same.

  Background documents and information:

  – *procedure for the selection of clearing and settlement providers.*

5.2.2 CLEARING AND SETTLEMENT PROVIDERS' FINANCIAL, OPERATIONAL AND SECURITY RISKS

Does the GA monitor the creditworthiness, operational reliability and security of clearing and settlement providers? Does the GA take action on the basis of the results of monitoring activities with regard to the creditworthiness, operational reliability and security of clearing and settlement providers?

(Clearing and settlement arrangements and systems which are already covered by oversight are excluded.)

- The GA monitors the creditworthiness of settlement providers or requires settlement agents to do so and takes action based on the results of this monitoring.

- If clearing providers engage in activities that represent financial risks, the GA monitors the creditworthiness of clearing providers or requires clearing agents to do so and takes action based on the results of this monitoring.

- The GA monitors the operational reliability and security of clearing and/or settlement providers or requires clearing and settlement agents to do so and takes action based on the results of this monitoring.

- The GA has defined a process to ensure that necessary actions are reported to the respective decision-making bodies in order to initiate remedial actions (e.g. changing the settlement agent, issuing recommendations to the providers, holding meetings).

  Background documents and information:

  – *analysis of the financial, operational and security risks of the CPSs of major clearing and settlement providers.*

5.3 DEFAULT ARRANGEMENTS

IF THERE ARE ARRANGEMENTS TO COMPLETE SETTLEMENT IN THE EVENT OF AN ISSUER DEFAULTING ON ITS OBLIGATIONS, IT MUST BE ENSURED THAT ANY RESULTING COMMITMENT BY AN ACTOR DOES NOT EXCEED ITS RESOURCES, POTENTIALLY JEOPARDISING THE SOLVENCY OF THAT ACTOR. THE CARD PAYMENT SCHEME MUST ALSO ENSURE THAT ACTORS ARE FULLY AWARE OF THEIR OBLIGATIONS UNDER ANY SUCH ARRANGEMENT, IN LINE WITH STANDARD 2.

5.3.1 ARRANGEMENTS FOR AN ISSUER DEFAULTING

Where arrangements are made to complete settlement in the event of an issuer defaulting, is it ensured that any resulting commitment on the part of the other settlement provider(s) does not exceed its resources?

(Settlement arrangements and systems which are already covered by oversight are excluded).

- The GA has a process in place to determine the resources needed, in principle, to complete settlement and to review the amounts on a regular/event-driven basis (e.g. given the calculated maximum likely exposure in the event of a participant default).

- The GA has set a procedure for the CPS to make the necessary resources available to complete settlement and to ensure that these resources are sufficiently liquid.

  Background documents and information:

  – *CPS's default arrangements to complete settlement (e.g. how are the required resources determined? How many are there and how liquid are they? Who decides what changes need to be made? Based on what criteria are these decisions taken?).*

  – *CPS's default policies and procedures (how will the resources be used in case of default and how will the burden of default be allocated after the available resources have been used up?).*

5.3.2 SETTLEMENT PROVIDERS' AWARENESS OF THEIR OBLIGATIONS

Does the GA have a procedure in place to ensure that all settlement providers participating in arrangements to complete settlement in the event of an issuer defaulting are aware of their obligations and comply with the relevant regulations regarding solvency?

- The GA has a procedure in place to inform and to make all settlement providers aware of their obligations and the potential size of such obligations to complete settlement in the event of an issuer defaulting. These obligations should be clearly defined in the system rules.

- The GA has the ability to check whether settlement providers are able to meet their obligations without jeopardising their own solvency.

  Background documents and information:

  – *CPS's procedures and rules regarding the settlement providers' awareness of their obligations.*

GLOSSARY

The following terms are defined for the purpose of this assessment guide.

Term	Definition
Acceptance	The process of checking whether the transaction complies with the CPS rules (e.g. the card has not expired or been revoked, the identity of the card and the cardholder is correct and the financial limits of the cardholder have not been exceeded).
Accepting device	Any device that processes payment card transactions where the card and cardholder are present.
Actors	The actors of the CPS are the governance authority, the issuers, the acquirer, technical service providers, the clearing provider, the settlement provider and the customers (cardholder and card acceptor).
Authentication	The methods used to verify the origin of a message or the identity of a participant connected to a system.
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
Authorisation	The process initiated by a point of sale (POS) or an automated teller machine (ATM) by which a request for the transfer of funds for the benefit of the card acceptor and ultimately paid for by the cardholder is approved or declined. In general, the decision to approve or decline a transaction is taken by the issuer or by a third party on behalf of the issuer.
Card acceptor (payee)	A retailer or any other entity, firm or corporation that enters into an agreement with an acquirer to accept payment cards, when properly presented, as payment for goods and services (including cash withdrawals) and which will result in a transfer of funds in its favour.
Card acquirer	A credit institution, payment service provider as defined in the Payment Services Directive or other undertaking that enters into a contractual relationship with a card acceptor and the card issuer via the CPS, for the purpose of accepting and processing card transactions. In some cases, the card acquirer may act as a card acceptor itself.
Cardholder (payer)	The person or entity that enters into an agreement with an issuer in order to obtain a payment card. Through this agreement, the cardholder is authorised to use the card for its intended purposes (e.g. payment guarantee, cash withdrawal, cheque guarantee, identification, multi-applications, etc.).
Card issuer	The credit institution (or more rarely another undertaking) that is a member of a card scheme and enters into a contractual relationship with a cardholder that results in the provision and use of a card of that CPS by that cardholder.
Card-not-present payment	A payment transaction based on card-related information without the card being physically presented to the merchant (e.g. mail order, telephone order, internet payments).
Card payment scheme (CPS)	For the purposes of the oversight framework, a card payment scheme is the set of functions, procedures, arrangements, rules and devices that enable a holder of a payment card to effect a payment and/or cash withdrawal transaction with a third party other than the card issuer. The oversight framework covers the entire payment cycle, i.e. the transaction phase (including the manufacture of payment instruments and the processing of data) and the clearing and settlement phase; it accommodates concerns relating to both the retail payment system and the payment instrument used.
Chargeback	A chargeback is a reversal of a card payment transaction (financial liability), in whole or in part, by the card issuer to the acquirer and, usually, by the acquirer to the card acceptor.
Clearing agent (operator of the clearing system)	The clearing agent is the operator of the clearing system (e.g. STET CORE, EQUENS).
Clearing arrangement	A clearing arrangement consists of a clearing system, as well as any contracts between CPS actors regarding the clearing of card transactions. The clearing system is a set of rules and procedures whereby financial institutions present and exchange data and/or documents relating to transfers of funds or securities to other financial institutions at a single location (e.g. a clearing house). These procedures often include a mechanism for calculating participants' mutual positions, potentially on a net basis with a view to facilitating the settlement of their obligations in a settlement system.
Clearing provider	The PSP providing clearing services to other market participants (e.g. a PSP having direct access to a clearing system).
Confidentiality	The quality of being protected against unauthorised disclosure.
Credentials	The information – generally confidential – provided by a customer or PSP for the purposes of authentication. Credentials can also mean the physical tool containing the information (e.g. one-time-password generator, smart card), or something the user memorises or represents (such as biometric characteristics).

Term	Definition
Cryptographic algorithm	A mathematical function that is applied to data to ensure confidentiality, data integrity and/or authentication. A cryptographic algorithm, using keys, can be symmetric or asymmetric. In a symmetric algorithm, the same key is used for encryption and decryption. In an asymmetric algorithm, different keys are used for encryption and decryption.
Cryptographic key	A mathematical value that is used in an algorithm to generate cipher text from plain text or vice versa.
Customers	The parties (cardholder and card acceptor) using the services of the CPS.
Governance authority	Term which refers to the actor(s) performing the governance functions described in the scheme's overall management sub-system. The actor performing governance functions is responsible for the functions it performs within the scheme and is the addressee of the standards in this respect. If there is more than one actor for a given scheme, they are jointly accountable for the overall functioning of the CPS, for promoting the payment instrument, for ensuring compliance with the scheme's rules and for setting clearly defined, transparent, complete and documented boundaries for their responsibilities within this scheme. These actors must then jointly ensure that all the relevant standards of this oversight framework are met. Oversight activities will be conducted taking into account the division of responsibilities. Nevertheless, all measures taken and all activities carried out within the scheme should be in line with the security policies defined by the actor(s) performing governance functions.
Financial risk	A term covering a range of risks incurred in financial transactions (e.g. liquidity and credit risks).
Integrity	The quality of being protected against accidental or fraudulent alteration or the quality of indicating whether or not alteration has occurred.
Major payment security incident	An incident which has or may have a material impact on the security, integrity or continuity of the PSP's payment-related systems and/or the security of sensitive payment data or funds. The assessment of materiality should consider the number of potentially affected customers, the amount at risk and the impact on other PSPs or other payment infrastructures.
Off-line transaction	A transaction processed and approved/declined at an accepting device on the basis of communication between the card and the accepting device without actually contacting the issuer (or its agent).
Online transaction	A transaction that is approved or declined at an accepting device following a real-time dialogue between the acquirer and issuer (or its agent). This requires that the accepting device is connected online during the transaction phase to the acquirer, to send the request and to receive the response.
Outsourcing	Outsourcing occurs when a service provider contracts a third party to fulfil its own responsibilities as defined by the CPS. In general, each service provider is fully responsible for all outsourced activities. Such a service provider must ensure that all outsourced services and activities are provided, managed and monitored in the same way as if they were operated by the service provider itself.
Payment card	A device that offers the ability to make payments for goods and services, either at an accepting device or remotely (via mail order, telephone order or the internet – these are known as "card-not-present" transactions), or to withdraw cash from an ATM.
Payment service providers (PSPs)	PSPs may be: (a) credit institutions; (b) electronic money institutions; (c) post office giro institutions; (d) payment institutions; (e) the European Central Bank and national central banks when not acting in their capacity as monetary authorities or other public authorities; and (f) Member States or their regional or local authorities when not acting in their capacity as public authorities. However, in addition, overseers might assess the services of other service providers with a different legal status if their services have an influence on the security of CPSs. Thus, with regard to the compliance with the oversight standards, there is no differentiation between the legal status of PSPs.
PIN (personal identification number)	A secret code which the cardholder may need to verify his/her identity.
Personalisation of a card	Writing and storing all of the information necessary on to a card for it to be used for payments or to obtain cash from an ATM.
Scheme	Refers to the card payment scheme.
Secret	Information which can only be known by or in the possession of (e.g. cryptographic key) the authorised users. This information is used to strenghthen security.
Sensitive information	Sensitive information is defined as any information where unauthorised access (including internally) may lead to considerable damage for individuals, entities and/or their interests. It includes sensitive payment data.

Term	Definition
Sensitive payment data	Sensitive payment data are defined as data which could be used to carry out fraud. These include data enabling a payment order to be initiated, data used for authentication, data used for ordering payment instruments or authentication tools to be sent to customers, as well as data, parameters and software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise electronic mandates or control the account, such as "black" and "white" lists, customer-defined limits, etc. An indicative list of elements that could, depending on the circumstances under which the data are used, be considered as sensitive payment data is provided below. The overseen entity should provide the overseer with a list of elements it considers as sensitive payment data; based on this, the overseer/supervisor will decide on a case-by-case basis taking into account the respective business models. a) The set of data enabling a payment order to be initiated, e.g.: - payment account identifiers of the customer stored at the PSP: IBAN (or equivalent). The BIC should not be considered as sensitive data; - payment card data: PAN, expiry date, CVx2; b) Data used for authentication (when applicable and used in this context), e.g.: - customer identifiers (e.g. client number/log-in name); - passwords, codes, PIN, secret questions, reset passwords/codes; - phone number (mobile or landline, when applicable); - certificates; c) Data used for ordering payment instruments or authentication tools to be sent to customers (in the case of a PSP offering this functionality online, otherwise these data are not considered as sensitive), e.g.: - client's postal address; - phone number, e-mail address; d) Data, parameters and software stored in the PSP's systems, which, if modified, may undermine the security of the delivery of payment instruments or authentication tools to the customer or may affect the latter's ability to verify payment transactions, authorise e-mandates or control the account, e.g.: - "black" and "white" lists, customer-defined limits, etc.; - data outlined in (a), (b) and (c) depending on applicability and the methods used.
Service providers	The actors who participate with internal or external resources in services offered to customers of the CPS. Service providers include: issuers; card manufacturers; acquirers; terminal manufacturers; maintenance operators; "switches" (transaction collectors which dispatch further information); communication network service providers; clearing providers (payment system operators); and settlement providers. In some cases, an entity may play different roles: for example, in the case of three-party schemes, the issuer and acquirer are the same entity. Given the relevance of issuing and acquiring in CPSs, this document often refers to "issuer" and "acquirer" as "participants".
Settlement agent (settlement institution, settlement bank)	The institution across whose books transfers between participants take place in order to achieve settlement within a settlement system (e.g. national central banks in the case of TARGET2).
Settlement arrangement	A settlement arrangement consists of a settlement system or standardised arrangements, as well as any contracts between CPS actors regarding the settlement of funds for card transactions. A settlement system is a system used to facilitate the transfer of funds, assets or financial instruments.
Settlement provider (settling participant, settlement bank, settling member)	An institution (e.g. a PSP) which maintains one or more accounts with a settlement agent in order to settle funds on its own behalf or, potentially, for other market participants.
Strong customer authentication	Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: (i) something only the user knows, e.g. static password, code, personal identification number; (ii) something only the user possesses, e.g. token, smart card, mobile phone; and (iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.
Switch	The routing centre that transfers authorisation requests, approvals and transaction information to the appropriate receiver.
Terminal	A type of accepting device.
Transaction phase	This phase encompasses the acceptance and authorisation of a card, as well as the exchange of the data used as an input for the clearing and settlement process.
Transaction risk analysis	Evaluation of the risk related to a specific transaction taking into account criteria such as customer payment patterns (behaviour), the value of the related transaction, the type of product and the payee profile.
Wallet solutions	Solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.