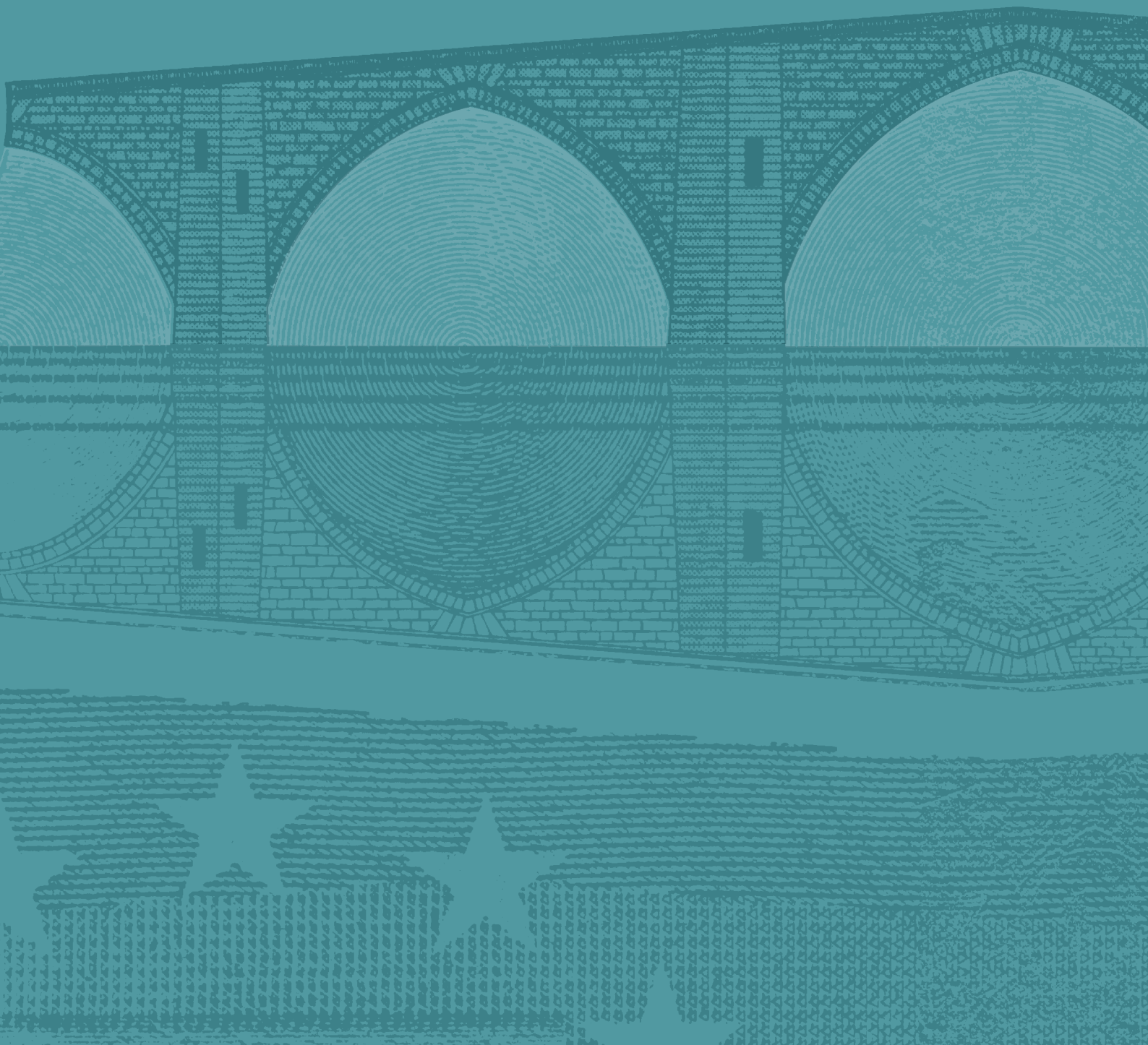
EUROPEAN CENTRAL BANK

EUROSYSTEM

GUIDE FOR THE ASSESSMENT OF DIRECT DEBIT SCHEMES AGAINST THE OVERSIGHT STANDARDS

NOVEMBER 2014



EUROPEAN CENTRAL BANK

EUROSYSTEM

In 2014 all ECB publications feature a motif taken from the €20 banknote.

GUIDE FOR THE ASSESSMENT OF DIRECT DEBIT SCHEMES AGAINST THE OVERSIGHT STANDARDS

NOVEMBER 2014

© European Central Bank, 2014

Address
Kaiserstrasse 29
60311 Frankfurt am Main
Germany

Postal address
Postfach 16 03 19
60066 Frankfurt am Main
Germany

Telephone
+49 69 1344 0

Website
http://www.ecb.europa.eu

Fax
+49 69 1344 6000

All rights reserved. Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged.

ISBN 978-92-899-1480-2 (online)
EU catalogue number QB-06-14-091-EN-N (online)
Digital object identifier: 10.2866/28762

CONTENTS

INTRODUCTION

The Eurosystem has developed oversight standards for direct debit schemes, with a particular focus on the security and efficiency of direct debit payments. This assessment guide supports a comprehensive and efficient assessment against these standards.

This assessment guide is intended both for the direct debit schemes' governance authorities (GAs) responsible for ensuring compliance, and for the overseers conducting the oversight of both national and international direct debit schemes based on the Eurosystem oversight standards for direct debit schemes. 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 direct debit schemes 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 direct debit schemes are expected to answer each of the AQs with a "Y" or "N", providing sufficient justification and evidence, and attaching supporting information and documents.

This assessment guide enables the overseers 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 direct debit schemes' level of observance for each of the oversight standards and will serve as a broad layout for the final oversight report.

The Eurosystem addresses its oversight standards to the governance authority of the direct debit scheme. The concept of **"governance authority"** with regard to direct debit schemes 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 direct debit scheme, 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.

Each scheme will be subject to a pre-assessment prior to the oversight assessment, in order to assess how governance authority roles are distributed. 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 direct debit scheme, the statistical information to be reported and 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 direct debit scheme. Although the AQs are very detailed, they should not be considered prescriptive as regards the organisation of the direct debit business. Indeed, the Eurosystem is aware that different options could be equally satisfactory in terms of reaching an acceptable level of resilience for each direct debit scheme 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. Moreover, it must be noted that a limited number of items refer to best practices outlined in the "Recommendations for the security of internet payments". Compliance with such best practices is not mandatory and will not be scored during the assessment process. The GA is nevertheless encouraged to indicate its compliance with them.

1 INFORMATION REQUIRED FROM DIRECT DEBIT 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 be in English. When this is not possible, a certified translation of the original or a copy of such a translation verified by the GA should be provided. Upon request, the GA has to submit the original of the document.

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 direct debit scheme 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 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 used;
- indicate when questions are not applicable and explain how it came to this conclusion.

1.4 STATISTICAL INFORMATION

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

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

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

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 direct debit scheme or one of its sub-systems described in Annex 1 of the "Direct debit scheme oversight framework – standards" (e.g. major network failure or a major fraud incident involving direct debit scheme data).

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

1.6 ESTABLISHMENT OF THE DIRECT DEBIT SCHEME

The direct debit scheme indicates its GA. The direct debit scheme 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 direct debit scheme 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 direct debit scheme 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;*

- *copy of the articles of association;*

- *information about the GA's registered branches and subsidiaries which are of relevance for the direct debit scheme business; extracts from the relevant commercial and public registers; the functions and responsibilities of the branches/subsidiaries;*

- *list of shareholders/partners and their shares/equity interests.*

1.7 STRUCTURE OF THE DIRECT DEBIT 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 direct debit scheme's management structure (e.g. head office and location(s) where the direct debit scheme'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 direct debit scheme; information about the direct debit scheme PSPs, technical service providers, as well as the clearing and settlement providers, and information on their roles, functions and responsibilities;*

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

1.8 DIRECT DEBIT SCHEME BUSINESS OVERVIEW

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

The following documents and information could be of relevance:

– *description of the direct debit scheme'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 direct debit scheme and other direct debit schemes, 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.).*

1.9 ACCESS CRITERIA

The GA should formulate direct debit scheme access criteria with sufficient levels of objectivity and ensure that the risks are managed with reasonable levels of due diligence and assurance.

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 a payee, payer, PSP, technical service provider, clearing provider or settlement provider;*

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

1.10 MANDATE HANDLING, INITIATION, ACCESS, TRANSACTIONS, CLEARING AND SETTLEMENT

The GA should ensure that it has envisaged a clear differentiation between platforms and processes for the clearing and settlement mechanisms employed by the direct debit scheme.

The following documents and information could be of relevance:

- *information on the initiation phase including the provision, processing, storage and flow of the direct debit mandate; description of the access phase, including the initiation of the direct debit collection, access channels for the initiation of the collection (technical aspects and service providers involved in the access to the scheme) and the related security measures;*

- *information on entities involved in clearing services;*

- *information on entities involved in settlement arrangements;*

- *whenever applicable, an indication of the use of interbank and on-us transactions and correspondent banking;*

- *information on the GA's functions 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, SEPA, EMEA (Europe, the Middle East and Africa), etc.).*

1.11 OUTSOURCING

The GA should provide information about the 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 DIRECT DEBIT SCHEMES AND OVERSIGHT GUIDELINES

1 THE DIRECT DEBIT SCHEME SHOULD HAVE A SOUND LEGAL BASIS UNDER ALL RELEVANT JURISDICTIONS

1.1 LEGAL FRAMEWORK

THE LEGAL FRAMEWORK GOVERNING THE ESTABLISHMENT AND FUNCTIONING OF THE DIRECT DEBIT SCHEME, THE RELATIONSHIP BETWEEN THE GA AND THE PAYEE'S PSP, THE PAYER'S PSP, THE PAYEE, THE PAYER AND THE OTHER SERVICE PROVIDERS[2], AS WELL AS THE RULES AND CONTRACTUAL ARRANGEMENTS GOVERNING THE DIRECT DEBIT SCHEME, SHOULD BE COMPLETE, UNAMBIGUOUS, UP-TO-DATE, ENFORCEABLE AND COMPLIANT WITH THE APPLICABLE LEGISLATION.

ESTABLISHMENT AND FUNCTIONING OF THE DIRECT DEBIT SCHEME

1.1.1 SCHEME ESTABLISHMENT

Are the rules governing the establishment and functioning of the GA compliant with the applicable national and EU legislation? Does the GA perform regular/event-driven reviews of this 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, 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 this 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 direct debit scheme and has done so when needed.

  Background documents and information:

  – *direct debit scheme's rules governing its establishment and functioning;*

  – *jurisdiction/law governing the establishment of the GA and the operation of the direct debit scheme (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 direct debit scheme (e.g. results, follow-up actions, experience gained, changes implemented, etc.);*

2 Communication network service providers, IT service providers, and clearing and settlement providers.

– *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 direct debit scheme (e.g. monitoring of legal developments, etc.).*

1.1.2 COMPLIANCE WITH LEGISLATION

Are the rules and procedures of the direct debit scheme compliant with any specifically applicable legislation? 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 the direct debit scheme rules with any specific legislation (e.g. the Payment Services Directive (PSD), Regulation (EC) No 924/2009, Regulation (EU) No 260/2012, anti-money laundering legislation[3]) relating to direct debits and/or to the electronic processing of payments in the countries where the direct debit scheme is operating.

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

- The GA requires the direct debit scheme actors 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:

  – *direct debit scheme's rules and procedures for direct debit payments and/or the processing of direct debit payments;*

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

  – *information on legal advice received;*

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

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

3 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.

1.1.3 COMPLETENESS, UNAMBIGUITY AND ENFORCEABILITY

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

- The GA has procedures in place to regularly ensure that the direct debit scheme'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);
  - 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 (e.g. for additional services) set by direct debit scheme 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 direct debit scheme for completeness, unambiguity and enforceability;*
  - *information on the most recent review of the direct debit scheme's rules and procedures (e.g. results, follow-up actions, experience gained, changes implemented, etc.);*
  - *direct debit scheme's policies ensuring that the rules and procedures set by the direct debit scheme service providers are compliant with the ones set by the GA and that they are complete, unambiguous and enforceable;*
  - *complaints from direct debit scheme 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.*

DIRECT DEBIT SCHEME ACTORS' RELATIONSHIPS

1.1.4 LEGALLY BINDING NATURE

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

- The GA requires direct debit scheme actors to ensure that:

  – the relationship between direct debit scheme actors in the different countries is contractually documented;

  – these contracts are signed and legally binding under the different laws of the countries where the direct debit scheme is operating.

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

  Background documents and information:

  – *contractual arrangements which govern the relationships between direct debit scheme 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 direct debit scheme operates;*

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

1.1.5 ACTORS

Are the relationships/contractual arrangements between direct debit scheme actors compliant with the applicable national and EU legislation? Do the direct debit scheme service providers perform regular/event-driven reviews of this compatibility?

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

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

- The GA requires the direct debit scheme actors 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 direct debit scheme service providers act accordingly;*

  – *information on the most recent legal advice received to test and ensure that the provisions of the contractual arrangements between direct debit scheme 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 among the direct debit scheme 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 direct debit scheme actors (and between scheme actors) 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 regarding 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 direct debit scheme actors comply 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 direct debit scheme service providers are compliant with the rules and procedures set by the GA and that they are complete, unambiguous and enforceable;*

  – *complaints from direct debit scheme 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 DIRECT DEBIT SCHEME

IF THE SCHEME OPERATES UNDER VARIOUS DIFFERENT JURISDICTIONS, THE LAW OF THESE JURISDICTIONS SHOULD BE ANALYSED IN ORDER TO IDENTIFY THE EXISTENCE OF ANY CONFLICTS. WHERE SUCH CONFLICTS EXIST, APPROPRIATE ARRANGEMENTS SHOULD BE MADE TO MITIGATE THE CONSEQUENCES OF THESE CONFLICTS.

1.2.1 GOVERNING LAWS, COURTS

Are the governing law(s) and the competent court(s) which are applicable to the relationships among the direct debit scheme actors clearly identified?

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

- The GA requires the direct debit scheme actors to have a similar procedure in place and to act accordingly.

  Background documents and information:

  – *procedures established to identify the different jurisdictions related to direct debit scheme contractual arrangements;*

  – *most recent legal advice received on contractual arrangements between direct debit scheme 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 CONFLICT OF LAW

Has the GA examined whether possible conflicts of law, having the potential to significantly impact the scheme, could arise between the different jurisdictions where the scheme operates? Once conflicts are 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 the different jurisdictions where the scheme operates and to assess the potential impact on the scheme (e.g. by classifying these conflicts according to 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 direct debit scheme 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 DIRECT DEBIT 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 DIRECT DEBIT 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 direct debit scheme 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 governance and functioning of the direct debit scheme.
- 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:

  – *direct debit scheme's rules and contractual arrangements related to the governance and functioning of the direct debit scheme;*

  – *information on the roles and responsibilities of all direct debit scheme 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 direct debit scheme 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 rules governing mandates and refund eligibility) 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 direct debit scheme for the announcement/ communication of any major changes.

  Background documents and information:

  - *procedures for 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 contract negotiation process?

- The GA produces or requires direct debit scheme PSPs to produce detailed statements (e.g. a brochure) about fee structures and fees (e.g. member access and annual fees, interchange fees, 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

ALL ACTORS (PAYEE'S PSP, PAYERS' PSP, PAYEES AND PAYERS) SHOULD HAVE ACCESS TO RELEVANT INFORMATION IN ORDER TO EVALUATE RISKS AFFECTING THEM, INCLUDING FINANCIAL RISKS. MOREOVER, SUFFICIENT INFORMATION SHOULD BE PROVIDED TO THE PAYERS BY OTHER ACTORS (E.G. PAYERS' PSPS AND PAYEES). IN PARTICULAR, PAYERS SHOULD BE AWARE OF THE DIRECT DEBIT TRANSACTIONS THEY AUTHORISE AND THE MANDATES THEY ISSUE, AND THEY SHOULD ALSO BE INFORMED APPROPRIATELY ABOUT COLLECTIONS.

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 payees' PSPs and payers' PSPs 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 payers and payees.

- This information includes descriptions of any liabilities or obligations that determine the allocation of financial risk.

- 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).

- 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;*

  – *direct debit scheme 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 RETURN AND FRAUD INFORMATION

Is sufficient and up-to-date information on returns and fraud (e.g. unauthorised direct debits) and the mitigation thereof available to actors and also to potential actors? Is the security awareness of direct debit scheme payers and payees 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 direct debits and mandates (e.g. cancellation of mandates, limits for the payment services provided, possibility to disable the internet payment functionality, blocking of direct debit transactions and refund rights).

- The GA requires that PSPs include clauses in their contracts with their customers 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 follow to reactivate the payment service;

  – the communication modalities between the customer and the PSP for unblocking a blocked service.

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

  – protect 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 payment website of the PSP.

- 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 the PSP has explained: (i) the procedure for customers to report (suspected) fraudulent payments, suspicious incidents or anomalies during the 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 returns, fraud activities and mitigation measures, the GA ensures that all relevant actors are informed.

  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.*

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

- The GA could require payees' PSPs 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 payees (i.e. a procedure is in place to track the number of merchants that attended courses and completed the programmes);

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

2.2.3 TIMING AND FREQUENCY

Are payers and payees appropriately informed about the timing and frequency of collections?

- The GA has set general rules for the execution times and frequencies of direct debit orders.
- The GA has set rules to inform the payers and payees about these execution times and frequencies.
- The GA has defined appropriate provisions (e.g. a policy for service providers, communication channels, etc.) for communication between actors that would be financially affected by significant disruptions in the functioning of a direct debit scheme.
- The GA requires that these provisions are followed by all service providers (e.g. via rules or service level agreements).

  Background documents and information:

  – *Information sent to customers about execution times and frequencies of direct debit orders.*

2.2.4 APPROPRIATE INFORMATION TO PAYERS

Are payers made aware of the implications of signing a mandate and authorising transactions? Are payers appropriately informed by their PSPs about preventive and corrective actions (e.g. cancellation of mandates, blocking of direct debit transactions and refund rights)?

- The GA has set general rules for payers' PSPs with the aim of informing payers 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 the payers' PSPs to supply payers, 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 direct debits over the internet. These should include, as appropriate:

  – clear information on any requirements in terms of payers' 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 payer to 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 payer;

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

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

– a description of the responsibilities and liabilities of the payer's PSP and the payer respectively with regard to the use of direct debits over the internet.

- The GA requires payers' PSPs to obtain from payers a formal acknowledgement of the receipt of this information.

- The GA requires payers' PSPs to include clauses in their contracts with their customers 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 modalities for communication between the cardholder and the issuer for unblocking a blocked service.

- The GA requires the payers' PSPs to:

  – inform payers of at least one secure channel (e.g. online banking, encrypted and digitally signed e-mail, dedicated secure website, ATM) for ongoing communication with payers regarding the correct and secure use of direct debits 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 internet 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 payers 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 payers in a transparent way that they may disable the internet payment functionality. The relevant procedure is efficient and clearly explained;

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

  Background documents and information:

  – *scheme rules on secure communication channels;*

  – *external audits.*

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

- The GA could require PSPs 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 PAYEES

Are payees made aware of the risks they face as a consequence of participating in the scheme, in particular the obligation to be subject to refunds?

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

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

  – clear information on any requirements for the payee'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 payee 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 payee;

  – the procedures to follow 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 follow if an abuse is detected or suspected;

  – a description of the responsibilities and liabilities of the PSP and the payee with regard to the use of direct debits over the internet.

- The GA requires payees' PSPs to obtain from payees a formal acknowledgement of the receipt of this information.

- The GA requires payees' PSPs to have a procedure in place determining how the payee 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 payees about the risks of participating in the scheme.*

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

3.1 SECURITY MANAGEMENT

3.1.1 RISK ANALYSIS RELATED TO SECURITY, OPERATIONAL RELIABILITY AND BUSINESS CONTINUITY SHOULD BE CONDUCTED AND KEPT UP TO DATE IN ORDER TO DETERMINE AN ACCEPTABLE LEVEL OF RISK AND SELECT ADEQUATE POLICIES AND APPROPRIATE PROCEDURES FOR PREVENTING, DETECTING, CONTAINING AND CORRECTING VIOLATIONS. COMPLIANCE WITH SUCH FORMALISED POLICIES SHOULD BE ASSESSED ON A REGULAR BASIS.

3.1.1.1 Risk analysis

Is a comprehensive ongoing risk analysis conducted by the GA and updated on a regular or event-driven basis, taking into account all the different risk profiles of the various direct debit scheme 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 direct debit scheme (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 analysis of the risks involved in the use of direct debits over the internet and related services, taking into account the risk profiles of the direct debit scheme service providers involved. It takes into account the technological solutions and platforms used, the application architecture and the programming techniques and routines.

- The GA has conducted a risk analysis for all types of direct debits (e.g. SDD Core, SDD B2B) and transactions (e.g. first, one-off, recurrent, final) supported by the direct debit scheme, including a reference to mandate management. As a result, the GA has defined and implemented security policies adapted to these various types of direct debits and transactions.

- 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 direct debit scheme 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.*

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 direct debit scheme? 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 security policies covering the appropriate domains including those relevant to the use of direct debits over the internet (e.g. security management; protection of sensitive data or devices – including relevant mandate-related date information – during the initiation and transaction phases, clearing and settlement; business continuity; outsourcing and incident monitoring).

- 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;

  – role 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[4]);

  – 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 direct debit scheme's security policies and operational service levels as well as other requirements linked to security.

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

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

4 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.

of the direct debit scheme[5] and encompasses the review of the impact of major incidents and major changes).

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

  Background documents and information:

  – *direct debit scheme's security policies and procedures;*

  – *direct debit scheme's security monitoring framework;*

  – *information on the process for assessing the implementation of the direct debit scheme'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 direct debit scheme 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.*

5 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 direct debit scheme? Are rules in place requiring direct debit scheme 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, 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 direct debit scheme, especially with regard to fraud techniques (both for internal and external fraud), the evolution of the characteristics and features of the instrument, optional services and the initiation channels (e.g. signature of electronic mandates by mobile phone, over the internet or at a terminal).
- The GA requires all direct debit scheme service providers (e.g. via contracts) to:
  - monitor new technological developments themselves, especially with regard to fraud techniques and the evolution of the characteristics and features of the instrument, optional services 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 OF ALL STAKEHOLDERS INVOLVED 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 SCHEME-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 direct debit scheme?

- 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 direct debit scheme service providers to document the roles and responsibilities of their staff and management.

  Background documents and information:

  – *direct debit scheme's operational, contingency and control procedures;*

  – *staff and management task descriptions.*

3.1.2.2 Staff trustworthiness

Is it ensured that sensitive operational activities (e.g. the management of personal data such as account identifiers or secret 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 personnel authorised to perform these activities, and has defined access rights accordingly.
- The GA requires direct debit scheme 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 the competences, skills and resources necessary for its staff and management to carry out their tasks. Related training (e.g. physical or virtual educational programmes) and policies are regularly updated to ensure that the content remains relevant to a dynamic security environment.
- The GA requires direct debit scheme 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 template.*

3.1.3 OPERATIONAL AND INCIDENT MANAGEMENT SHOULD BE CLEARLY DEFINED AND EFFECTIVELY IMPLEMENTED. AS PART OF THIS OPERATIONAL MANAGEMENT, FRAUD SHOULD BE MONITORED EFFECTIVELY.

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 and made available such that the direct debit scheme 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 direct debit scheme. 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 frauds.

- The GA requires the direct debit scheme service providers to do likewise.

  Background documents and information:

  – *operational processes and equipment of particular importance for the functioning of the direct debit scheme;*

  – *information on major incidents affecting operational reliability, security breaches or 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 direct debit scheme, 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 direct debit scheme service providers), which are periodically reviewed and tested. These procedures include, where deemed relevant, clearly defined communication channels with all direct debit scheme service providers, so that incidents can be handled efficiently.

- The GA requires the direct debit scheme service providers to have incident management and escalation procedures in place, with clearly defined communication channels with the other direct debit scheme service providers and the GA (where 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 PSPs to contractually require payees that store, process or transit 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. PSPs have a procedure in place to ensure that even in the event of a major incident appropriate information is communicated to customers.

  Background documents and information:

  – *information on the most recent review of the direct debit scheme'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 direct debit scheme 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 direct debit scheme 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 direct debit scheme 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 and 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 services providers to do likewise for both requirements above.

- The GA periodically reviews and updates the change management process, and communicates any changes to all direct debit scheme service providers affected. The GA requires 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:

  – *direct debit scheme's 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 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 direct debit scheme service providers have equivalent control functions and procedures in place.

  Background documents and information:

  – *Access policies and procedures.*

3.1.4 THE SCHEME'S SECURITY POLICIES SHOULD ENSURE THE PRIVACY, INTEGRITY AND AUTHENTICITY OF DATA AND THE CONFIDENTIALITY OF SECRETS (WHERE APPLICABLE, E.G. FOR ELECTRONIC MANDATES) DURING THE INITIATION PHASE AND THE TRANSACTION PHASE, WHENEVER DATA ARE PROCESSED, STORED OR EXCHANGED. EFFECTIVE CONTINGENCY PLANS SHOULD BE IN PLACE IN CASE CONFIDENTIAL INFORMATION IS REVEALED OR COMPROMISED.

3.1.4.1 Protection of sensitive payment data

Are sensitive payment data identified, managed and adequately protected?

- The GA has a procedure to identify and list all elements it considers as sensitive payment data according to their protection needs.

- The GA requires direct debit scheme service providers to have relevant controls to ensure the proper protection of sensitive payment data.

- The GA requires direct debit scheme 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 requires PSPs to ensure that all sensitive payment data accessible to payers and payees 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 requires that payees 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.

- The GA requires PSPs to have set up a procedure to monitor compliance with this contractual obligation, specifying the steps to be taken in case of detected breaches, up to the termination of the payee's contract.

  Background documents and information:

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

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

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

- The GA could require PSPs to ensure that, if payees 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

Are the privacy, integrity and authenticity of data (including payers' personal data and mandate-related data) and the confidentiality of secrets (e.g. authentication and authorisation credentials) maintained where such data are processed, stored and exchanged?

- The GA has appropriate security solutions in place or requires direct debit scheme 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 for the development of 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 is maintained within the direct debit scheme during operation, storage and exchange.

- The GA tests and requires direct debit scheme service providers to test security measures for the use of direct debits 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 direct debit scheme service providers implement IT environment segregation (e.g. of the development, test and production environments). To do so, the direct debit scheme service providers may consider the following non-exhaustive list of issues:

  – 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 direct debit scheme service providers to do the same.

3.1.4.3 Secure communication

Is there a policy in place to ensure secure communication between all the actors?

- The GA has set up or requires direct debit scheme 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[6] 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.

- In case of non-compliance by the direct debit scheme service providers, the GA has taken measures to enforce the contractual obligation or terminate the contract.

  Background documents and information:

  – *policy on secure communication;*

  – *contracts.*

3.1.4.4 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[7]) to be used within the direct debit scheme;

  – 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 secret information. The GA accordingly updates its set of algorithms and key lengths to be used within the direct debit scheme. The GA has a procedure in place to ensure that all direct debit scheme service providers adapt accordingly.

  Background documents and information:

  – *list of recommended cryptographic algorithms;*

6 The encryption should cover the whole communication session ("full session encryption").
7 In this context, the term "entropy" means a measure of the amount of uncertainty that an attacker faces to determine 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.

– *password policy;*

– *report on the use of cryptographic algorithms and passwords by service providers.*

3.1.4.5 Compromised secrets

Is there a contingency plan in place outlining the 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 outlining the procedures to be followed in the event of secrets being compromised.

- 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 direct debit scheme service providers. It is documented, tested and reviewed on a regular basis.

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

3.1.5 EXPLICIT POLICIES FOR CONTROLLING BOTH PHYSICAL AND LOGICAL ACCESS TO DIRECT DEBIT PROCESSING SYSTEMS AND LOCATIONS MUST BE DEFINED AND DOCUMENTED. ACCESS RIGHTS MUST BE USED IN A RESTRICTIVE WAY.

3.1.5.1 Access policy

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

- The GA has identified the staff members responsible for direct debit scheme 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 direct debit scheme service providers have a similar identification and access policy in place.

- These requirements include that:

  – Access privileges (including for administrators, super users/roots, 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[8] 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.*

3.1.5.2 Access procedure transparency

Are access procedures explicitly documented, made available to all direct debit scheme actors concerned and regularly updated?

- The GA has formalised and documented its access procedures and communicated them to all direct debit scheme actors concerned.
- The GA ensures that all these procedures are updated on a regular basis.
- The GA requires service providers to do likewise.

Background documents and information:

– *communication policy on access procedures;*

– *list of the last updates of these procedures.*

3.1.5.3 Access testing

Is the proper implementation of access procedures regularly tested and monitored?

- The GA regularly tests and monitors the proper implementation of its access procedures.
- The GA requires that direct debit scheme service providers test and monitor the proper implementation of their access procedures (e.g. via contractual requirements).

8 "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, pp. 388.

Background documents and information:

– *Results of the last tests and monitoring of the access procedures.*

3.2 SECURITY THROUGHOUT THE DIFFERENT PHASES (ACCESS, INITIATION, TRANSACTION)

3.2.1 ADEQUATE SECURITY REQUIREMENTS SHOULD BE DEFINED AND ENFORCED FOR THE ACCESS OF ACTORS SUCH AS PAYEES TO THE SCHEME, THE INITIATION PHASE (INCLUDING THE OPTION TO USE ELECTRONIC MANDATES AND THE CANCELLATION OF MANDATES) AND THE TRANSACTION PHASE (INCLUDING R-TRANSACTIONS).

3.2.1.1 Scheme security measures

Does the GA define security measures in line with the scheme's security policy (e.g. for mandate management, collections and R-transactions and for checking the authenticity and the validity of credentials and authentication devices, networks, websites, servers communication channels and protocols)?

- The GA has defined security specifications for each transaction type used within the direct debit scheme, and these are in line with the scheme's security policy. These specifications ensure, for example, that:

  i) the issuance or amendment of electronic mandates is protected by strong customer authentication when a PSP is involved in the process[9];

  ii) the access to sensitive payment data is protected by strong customer authentication;

  iii) the direct debit scheme ensures proper bilateral authentication when communicating with payees for the purposes of initiating direct debit collections on the internet and accessing sensitive payment data (e.g. through the use of secure protocols (e.g. TLS) allowing mutual authentication according to current best practices (e.g. key length, TLS version, encryption cipher, etc.));

  iv) the authenticity and validity of authentication means (e.g. physical or electronic signatures, passwords, cryptographic keys, tokens, biometrics) and the accepting system (e.g. bank server or payee server) are checked before a mandate or a transaction is accepted.

- The GA requires all direct debit scheme PSPs to act in the same manner.

Background documents and information:

– *list of security specifications;*

– *description of the alternative customer authentication measures;*

– *audits and issued recommendations.*

9 Alternative customer authentication measures may be considered by PSPs for the issuance or amendment of electronic mandates when the debtor and creditor accounts are held by the same customer.

3.2.1.2 Secrets and authentication devices

Does the direct debit scheme define procedures for the secure management of secrets (e.g. passwords, cryptographic keys), as well as security requirements for authentication procedures and related devices (e.g. tokens, cryptographic devices)?

- The GA has defined secure policies and procedures for managing secrets and authentication tools within the direct debit scheme and requires all direct debit scheme service providers to both comply with these requirements and ensure that their customers which are payees do so as well. This includes procedures for strong customer authentication, for password management and for the whole life cycle of cryptographic keys (e.g. generation, distribution, loading, storage, usage, backup/recovery, destruction and compromise).

  Background documents and information:

  – *procedure for managing secrets and authentication means;*

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

  – *audits and issued recommendations.*

3.2.1.3 Authentication procedure

Does the scheme require PSPs 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[10];

  – the security features of the solution (e.g. algorithm specifications, key length, information entropy) are properly defined and implemented and, in particular, 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;

  – measures to mitigate risks (e.g. of malware infection or hacking attacks) related to 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 a one-time password or initiate a drop call mechanism). Such measures could follow publicly available and recognised standards or 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, it is ensured that the likelihood of a false positive is comparable to or less than that for a (sound) password;

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

– 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 combined with an ownership element, 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[11];

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

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 payee, 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.

11 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.

3.2.1.4 Evaluation of devices and procedures

Do independent and competent third parties evaluate both the electronic devices given to payers and payees and authentication procedures?

- The GA has defined or requires PSPs to define a formal approval procedure for the use of electronic components (e.g. tokens) and devices (e.g. accepting devices) given to payers and payees and, in particular, for the strong 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 certify or evaluate 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:

  – *list of the devices given to payers and payees to operate strong customer authentication;*

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

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

3.2.1.5 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 internet payment service and/or the delivery of payment-related software to customers is carried out in a secure manner?

- The GA requires that PSPs:

  – implement a procedure ensuring that the enrolment for and provision of authentication tools and/or the delivery of payment-related software to the customer take 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 internet 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.

Background documents and information:

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

3.2.1.6 Validity periods

Are clear validity periods defined for authentication devices and secrets?

- The GA has defined and/or requires PSPs to define policies regarding appropriate validity periods for authentication devices and secrets (including OTPs[12]) 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 and ensure that their customers which are payees do so as well, including payees offering electronic mandate services to debtors.

Background documents and information:

– *general policies on expiry dates and secret information;*

– *contractual clauses on expiry dates and secret information;*

– *audits and issued recommendations.*

3.2.1.7 Access phase

Does the direct debit scheme define adequate procedures related to the access of actors to the scheme? Are these procedures adequate to ensure the authentication of all parties, to prevent the unauthorised use of payment services and to control access based on actors' roles?

- The GA has defined procedures governing payees' and payers' access to the scheme which cover:

  i) customers' initial registration and appropriate identification prior to being granted access to the use of direct debits over the internet (i.e. where the customer is not identified in a face-to-face environment, the customer's information is checked with and confirmed by reliable third-party information[13]);

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

13 Depending on the respective national legislation, this might be e.g. telephone/electricity bills, identification by third parties, or information gathered on the basis of a bank transfer of a small amount.

ii) the PSPs' procedures for customer due diligence, which are reviewed periodically by an internal/external auditor and reported to the Board and to the competent authority;

iii) the delivery of security devices or secrets for the authentication of the payees and payers involved (e.g. separate delivery of devices and credentials, separate delivery channels);

iv) the access management for e-banking services or other procedures to access sensitive applications (e.g. account management, payment-related software, remote payment orders, storage of private data);

v) the management of electronic mandates via public networks (e.g. web applications).

- The GA has defined security requirements ensuring that the actors' means of authentication are: (i) checked (before granting access) to verify that they have been correctly used and do not appear to be stolen or counterfeited (e.g. separate delivery of personalised security credentials, firewalls with appropriate rules to allow only legitimate connections); and (ii) protected against possible attacks (e.g. in providing security tools[14] to protect the customer interface against unlawful use or attacks), such as eavesdropping, cracking, phishing/pharming and social engineering.

- The GA has defined security requirements ensuring that access to the direct debit scheme services is granted based on actors' roles.

- The GA requires all direct debit scheme service providers to have contractual arrangements with payers, payees or PSPs obliging them to comply with these requirements and to have the ability to check whether payees act accordingly.

Background documents and information:

– *list of security requirements for the access phase;*

– *procedures governing actors' access to the scheme;*

– *contracts and in particular clauses on the access phase;*

– *audits and issued recommendations.*

3.2.1.8 Initiation phase

Does the direct debit scheme define and enforce secure procedures related to the creation, amendment, retrieval, expiration and cancellation of mandates, in line with the direct debit scheme's security policies, which aim to ensure: (i) the authentication of direct debit scheme payers and payees; (ii) the non-repudiation of a transmission/reception; and (iii) the integrity and confidentiality of the mandate itself and the related data? Has the GA implemented a change in liability in the payment scheme to support strong customer authentication when generating an electronic direct debit mandate?

14 E.g. a secure interface provided by customised software running from a secure USB device or dedicated security software for screening the customer's computer.

- The GA has defined requirements in its direct debit scheme's security policy governing the initiation phase of direct debit payments, focusing on payers, payees and their PSPs. These requirements are related to the creation, amendment, copy retrieval and cancellation of mandates and aim to ensure:

  – the authentication of payers, i.e. the use of strong customer authentication for both the issuance and the amendment of electronic mandates when a PSP is involved in the issuance process and for the customer's establishment or modification of its list of authorised/blocked payees (i.e. white/black list provided for in Article 5.3(d) of Regulation (EU) No 260/2012);

  – the non-repudiation of a transmission/reception;

  – the integrity and confidentiality of the mandate itself and the related data.

- The GA requires all PSPs to have contractual arrangements with their customers obliging them to comply with these requirements. Where no PSP is involved in the issuance or amendment of electronic direct debit mandates, the payee's PSP could encourage its customers to implement a procedure using strong customer authentication.

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

- The GA has implemented a "liability shift" to support strong customer authentication for the issuance and amendment of electronic mandates. This liability regime is transparent, clear and enforceable and includes a dispute resolution mechanism.

  Background documents and information:

  – *security policy governing the initiation phase;*

  – *contractual clauses on the initiation phase and the separation of payment-related processes on payees' websites;*

  – *audits and issued recommendations.*

3.2.1.9 Transaction phase

Does the direct debit scheme define and enforce secure procedures for the payer-to-PSP and payee-to-PSP spheres related to the execution of direct debit payments, starting from the collection initiated by the payee up to the conclusion of the transaction? Do these secure procedures cover R-transactions, from initiation to conclusion?

- The GA has defined security requirements ensuring that the scheme's PSPs do not process fraudulent or unauthorised direct debit transactions (e.g. collections, R-transactions) initiated by payees.

- The GA has defined security requirements ensuring that payers and payees do not receive information that is fraudulent or has been tampered with from the direct debit scheme service providers.

- The GA requires that: (i) PSPs' blocking of transactions is supported by well-defined criteria (e.g. a risk matrix, taking into account the risk and general profile of a customer and the amounts involved in a particular transaction or the customer's payment behaviour); (ii) the procedure for unblocking transactions is in accordance with the PSD; (iii) PSPs inform their customers about costs and contributions as well as the possibility to present claims in case of an inappropriately blocked transaction.

- The GA has defined requirements ensuring the secure execution of direct debit transactions, starting from the collection initiated by the payee up to the conclusion of the transaction. These security requirements also cover R-transactions, from initiation to conclusion.

- The GA requires all direct debit scheme service providers to comply with these policies.

  Background documents and information:

  – *list of security requirements for the transaction phase;*

  – *contractual clauses on the transaction phase;*

  – *audits and issued recommendations.*

3.2.1.10 Detection of unauthorised activities

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

- The GA has defined a requirement in its direct debit scheme security policy governing the detection of unauthorised activities in relation to transaction and mandate data.

- The GA's or the direct debit scheme 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 and mandate 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 and mandate data. This requirement includes the obligation to identify the originator of the unauthorised activity. The log files are tamperproof 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 takes 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 and mandate data.

- The GA requires all direct debit scheme 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 and mandate data for inconsistencies, signs of tampering and unauthorised access).

  Background documents and information:

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

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

  – *audits and issued recommendations.*

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

- The GA could require a payee's PSP to contractually require its payees who store payment information to have adequate processes in place to support traceability and report relevant issues to the said PSP.

3.2.2 EFFECTIVE AND SECURE PROCEDURES SHOULD COVER ELECTRONIC MANDATES AND THE DEMATERIALISATION OF PAPER MANDATES.

3.2.2.1 Mandate dematerialisation

Does the direct debit scheme define and enforce secure procedures related to the dematerialisation of paper mandates, aimed at ensuring that the dematerialised mandate data are accurate and consistent with the content of the original mandate data?

- The GA has defined requirements related to the dematerialisation of paper mandates which aim to ensure that the dematerialised mandate data are accurate and consistent with the content of the original mandate data.

- The GA requires all direct debit scheme service providers to comply with these requirements and ensure that their customers which are payees do so as well.

  Background documents and information:

  – *list of requirements governing mandate dematerialisation;*

  – *contractual clauses on mandate dematerialisation;*

  – *audits and issued recommendations.*

3.2.2.2 Electronic mandate services

Whenever electronic mandate services are available to the direct debit scheme payers and payees, does the scheme define and enforce secure procedures aimed at ensuring that: (i) the mandate data electronically stored are accurate and consistent with the original electronic mandate digitally signed by the payer; and (ii) the payment collection data are consistent with the electronically stored mandate data?

- For payees and direct debit scheme service providers which offer electronic mandate services, the GA has defined secure procedures aiming to ensure that: (i) the electronically stored mandate data are accurate and consistent with the original electronic mandate digitally signed by the payer; and (ii) the payment collection data are consistent with the electronically stored mandate data.

- The GA requires all direct debit scheme service providers to follow these procedures and ensure that their customers which are payees do so as well.

  Background documents and information:

  – *policy to ensure the alignment of stored mandate and collection data with original electronic mandates;*

  – *audits and issued recommendations.*

3.2.3 THE ACTIVITIES OF PAYERS AND PAYEES SHOULD BE ADEQUATELY MONITORED IN LINE WITH THE SCHEME'S SECURITY POLICY 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.

3.2.3.1 Fraud monitoring

Has the direct debit scheme put in place an adequate suspicious transactions and fraud monitoring framework, in line with and linked to the risk analysis?

- The GA has defined the various types of suspicious transactions and fraud within the direct debit scheme.

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

- The GA requires direct debit scheme service providers 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 direct debit scheme.

- The GA requires the payer's PSP to be able to detect fraud and have fraud prevention solutions in place that use parameterised rules (e.g. black lists of compromised accounts or data breaches, potentially abnormal payee behaviour), 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 payees' PSPs to have fraud detection solutions implemented in such a way to allow monitoring of payees' activities on the basis of transaction patterns (e.g. transaction amounts and numbers), payees' categories or 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;*

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

– *audits and issued recommendations.*

3.2.3.2 Fraud response

Is the direct debit scheme 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 direct debit scheme.
- 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 direct debit scheme service providers to follow these procedures.

Background documents and information:

– *report on the financial impact of fraud within the direct debit scheme;*

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

– *contractual clauses on fraud response;*

– *audits and issued recommendations.*

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

- The GA could require PSPs 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 PSP's risk management policy.

3.2.3.3 Fraud impact mitigation

Does the direct debit scheme define security measures to mitigate the impact of fraud in line with the security policy? Are security measures in place (e.g. suspension of account access, rapid change of secrets or transaction limits)?

- The GA requires that the payer's PSP has conducted an analysis regarding the impact of fraud and has defined adequate security policies and measures for fraud mitigation. These include vto disable the use of direct debits 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) and a mechanism to prevent double log-in. The GA requires that PSPs have defined specific secure procedures to reactivate the use of direct debits over the internet.

- The GA requires payers' PSPs 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 direct debit collection initiated on 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 use of direct debits over the internet.

  Background documents and information:

  – *security policies and fraud mitigation procedures;*

  – *appropriate contractual clauses;*

  – *audits and issued recommendations.*

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

- The GA could require payers' PSPs to:

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

  – enable their customers to specify, in a safe and trusted environment, personalised rules as parameters for their behaviour with regard to their signature of direct debit electronic mandates and related services (e.g. that they will only sign electronic mandates from specific countries and that electronic mandates signed from elsewhere should be rejected).[15] 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 their online banking. Moreover, they should notify their customer of any changes made to the limits via an out-of-the-band channel (e.g. SMS alerts).

15 This requirement only applies to PSPs involved in the electronic mandate issuance process.

3.2.4 APPROPRIATE ARRANGEMENTS SHOULD BE MADE TO ENSURE THAT DIRECT DEBITS CAN BE PROCESSED AT ALL TIMES, EVEN ON PEAK DAYS.

3.2.4.1 Capacity monitoring

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

- The GA has identified and classified all sensitive operations related to transaction processing (e.g. the collection process).
- The GA has put in place procedures to monitor the traffic flows, capacity and performance of those operations and the GA requires direct debit scheme 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.*

3.2.4.2 Capacity planning

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

- The GA has defined or requires direct debit scheme service providers to define a procedure to periodically assess their processing capacity and, if relevant, to analyse the causes of potential disruptions and to initiate remedial actions. The goal of this procedure is to avoid systemic disruptions to direct debit 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.*

3.2.5 SUFFICIENT EVIDENCE SHOULD BE PROVIDED TO ENABLE TRANSPARENT AND EASY CLARIFICATION OF DISPUTES REGARDING PAYMENT TRANSACTIONS BETWEEN ACTORS.

3.2.5.1 Dispute resolution evidence

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

- The GA has defined the evidence that should be provided to demonstrate the validity of mandates and transactions and to enable disputes to be resolved.
- The GA requires direct debit scheme service providers to implement procedures to collect this evidence and provide it upon request.

Background documents and information:

– *List of the pieces of evidence to be provided to demonstrate the validity of mandates and transactions.*

3.3 CLEARING AND SETTLEMENT

3.3.1 CLEARING AND SETTLEMENT ARRANGEMENTS SHOULD ENSURE AN ADEQUATE DEGREE OF SECURITY, OPERATIONAL RELIABILITY AND AVAILABILITY, TAKING INTO ACCOUNT THE SETTLEMENT DEADLINES SPECIFIED BY THE DIRECT DEBIT SCHEME.

3.3.1.1 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 direct debit scheme?

- 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[16], taking into account specified settlement deadlines. These requirements include measures relating to capacity, availability, confidentiality, auditability, integrity and authenticity.

- The GA requires direct debit scheme 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.*

3.3.1.2 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 direct debit scheme's requirements.

- The GA could consider assessments or activities carried out as part of supervision of payment service providers.

16 The monitoring of the operational reliability of clearing and settlement agents is covered by assessment questions 5.1.6 and 5.1.7.

Background documents and information:

– *Audits and issued recommendations.*

3.3.1.3 Unavailability and reliability problems

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

(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 processes is provided).

  Background documents and information:

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

  – *audits and issued recommendations.*

3.4 BUSINESS CONTINUITY

3.4.1 THE SCHEME'S BUSINESS IMPACT ANALYSES SHOULD CLEARLY IDENTIFY THE OPERATIONS THAT ARE CRUCIAL FOR THE SMOOTH FUNCTIONING OF THE DIRECT DEBIT SCHEME. EFFECTIVE AND COMPREHENSIVE CONTINGENCY PLANS SHOULD BE IN PLACE IN THE EVENT OF A DISASTER OR ANY INCIDENT THAT JEOPARDISES THE AVAILABILITY OF THE SCHEME. THE ADEQUACY SHOULD BE TESTED AND REVIEWED REGULARLY.

3.4.1.1 Business continuity plans

Has the direct debit scheme identified the operations that 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 operations which are essential to the smooth functioning of the direct debit scheme (e.g. authorisation and processing of transactions).

- The GA has defined a service level necessary for the smooth functioning of the direct debit scheme.

- The GA has defined or requires service providers to define business continuity plans, including contingency processing arrangements, in line with the security policy and the agreed service level.

- 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 direct debit scheme service providers to define appropriate business continuity plans, including contingency processing arrangements, in line with the security policy for the direct debit scheme and the agreed direct debit scheme service level(s).

  Background documents and information:

  – *lists of the components and processes essential to the smooth functioning of the direct debit scheme;*

  – *direct debit scheme'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;*

  – *direct debit scheme's crisis management and crisis communication management arrangements.*

3.4.1.2 Business continuity testing

Are the effectiveness and adequacy of the business continuity plans tested and reviewed on a regular basis and/or in response to events?

- 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 supervision of payment service providers). These reviews include the testing, updating and communication of business continuity plans.

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

  Background documents and information:

  – *Audits and issued recommendations.*

3.5 OUTSOURCING

3.5.1 SPECIFIC RISKS RESULTING FROM OUTSOURCING SHOULD BE MANAGED WITH COMPLETE AND APPROPRIATE CONTRACTUAL PROVISIONS. THESE PROVISIONS SHOULD COVER ALL RELEVANT ISSUES FOR WHICH THE ACTOR WHO OUTSOURCES ACTIVITIES IS RESPONSIBLE WITHIN THE SCHEME.

3.5.1.1 Outsourcing risk analysis

Does the direct debit scheme analyse specific risks relating to outsourcing and their impact?

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

- The GA requires direct debit scheme service providers to do the same.

- The GA analyses risks and impacts for the direct debit scheme 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 and whether outsourcing risks may arise owing to reliance on a limited number of outsourcing partners and the possible implications that this could have on the service level agreements.

- The GA requires direct debit scheme service providers to analyse their specific risks and their impact related to these outsourcing activities.

- The GA could consider assessments or activities carried out as part of supervision of payment service providers.

  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.*

3.5.1.2 Contractual provisions

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

- 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 respects 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 direct debit scheme service providers to also obtain legal advice about the coverage of all outsourcing activities in their contractual provisions.

- The GA could consider assessments or activities carried out as part of supervision of payment service providers.

  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 direct debit scheme operates;*

  – *contractual clauses on outsourcing.*

3.5.1.3 Service level agreement and liabilities

Does the GA have contractual provisions in place 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 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 (including in the event of an emergency).
- The GA requires PSPs to do the same.
- The GA could consider assessments or activities carried out as part of supervision of payment service providers.

  Background documents and information:

  – *list of outsourcing partners;*

  – *contracts signed with outsourcing partners;*

  – *audits and issued recommendations.*

3.5.2 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 APPLICABLE WITHIN THE SCHEME.

3.5.2.1 Monitoring

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

- The GA has a process in place to monitor the security, availability and performance of outsourcing partners in line with the respective contracts.
- The GA requires direct debit scheme service providers to have the same process.
- The GA could consider assessments or activities carried out as part of supervision of payment service providers.

  Background documents and information:

  – *Report on outsourced activities.*

3.5.2.2 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 direct debit scheme, 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 direct debit scheme 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 DIRECT DEBIT SCHEME SHOULD HAVE EFFECTIVE, ACCOUNTABLE AND TRANSPARENT GOVERNANCE ARRANGEMENTS

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

– MAKING DECISIONS ABOUT BUSINESS OBJECTIVES AND POLICIES, INCLUDING ACCESS POLICIES

4.1.1 ROLES AND RESPONSIBILITIES IN DECISION-MAKING

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

- The GA has identified the roles and responsibilities of direct debit scheme 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 fulfil their roles and responsibilities 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, 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 direct debit scheme?

- The GA has defined the direct debit scheme 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 size of the direct debit scheme (taking into account all functions and the number of actors), its complexity (e.g. types of actors, licensees, etc.), its structure (e.g. national/Europe-wide/worldwide, type of company and law applicable, etc.), its economic significance (e.g. market share, basic accounting data, etc.) and 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 direct debit scheme 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 direct debit scheme's decision-making process.*

4.1.3 ACCESS POLICIES

Is access to the direct debit scheme 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 termination of and exit from the scheme clearly defined and transparent to the relevant service providers?

- The GA has set rules regarding access to the scheme (e.g. entry fees, financial stability, technical capacity, legal conformity) on the basis of fair, non-discriminatory criteria. Restrictive access criteria need to be justified (e.g. security considerations).

- The GA communicates its access policies to actors and potential actors, including any 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 termination of and exit from the scheme.

  Background documents and information:

  – *direct debit scheme's access policy;*

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

4.1.4 CONSULTATION OF ACTORS

Are the relevant direct debit scheme actors consulted during the decision-making process as regards major changes (e.g. changes concerning technology, liability, company structure, multilateral interchange fees or scheme rules)?

- The GA has defined a classification for changes based on their significance.
- For major changes (e.g. concerning technology, liability, company structure, multilateral interchange fees, rules, etc.), all the relevant direct debit scheme 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:

  – *direct debit scheme's classification for changes based on their significance;*

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

– **REVIEWING PERFORMANCE, USABILITY AND CONVENIENCE OF THE DIRECT DEBIT SCHEME**

4.1.5 REVIEW OF SERVICES

Are there adequate processes in place to analyse the performance, usability and convenience of the services offered to payers and payees by the direct debit scheme?

- The GA has a process in place to review the performance of the services offered to payers and payees 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 payers and payees by the direct debit scheme service providers.
- The GA requires PSPs to do the same.

  Background documents and information:

  – *direct debit scheme's customer satisfaction analysis/report;*

  – *direct debit scheme's performance, usability and convenience review.*

– IDENTIFYING, MITIGATING AND REPORTING SIGNIFICANT RISKS TO THE SCHEME'S OPERATION

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 direct debit scheme service providers are involved, the GA requires them to act in the same manner.

Background documents and information:

– *risk management process;*

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

– *audits and issued recommendations.*

4.2 INTERNAL CONTROL FRAMEWORK

THERE SHOULD BE 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 direct debit scheme? Does the GA monitor the implementation of audit requirements within the scheme?

- The GA has an internal control framework in place for the direct debit scheme 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.
- The implementation and functioning of the payment services as well as the PSP/GA's security measures are periodically audited in order to ensure their robustness and effectiveness. The audit upon the initial implementation is considered a one-off audit and further functional audits should be performed for major changes. The GA takes into consideration the security risks involved to determine, in proportion to the security risks, the frequency and focus of the audits.
- 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 direct debit scheme'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 direct debit scheme's control functions (e.g. appropriate level of reporting, internal/external audit)?

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

- 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 direct debit scheme service providers to have similar procedures in place.

  Background documents and information:

  – *rules and policies governing the direct debit scheme's audit function;*

  – *direct debit scheme'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 in determining the frequency and focus of audits.

- The GA has a procedure in place for immediate reporting when serious deviations from the direct debit scheme rules or other irregular events are detected (in case of external auditors, this is ensured in the contractual provisions). The GA requires direct debit scheme service providers to comply with these procedures. The GA can ask for audit reports from direct debit scheme service providers on issues pertaining to contracts, 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 PSPs to carry out regular checks for those payees 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 payee, the PSP can take measures to enforce the contractual obligation or terminate the contract.

Background documents and information:

– *procedures for reviewing the effectiveness of the control framework;*

– *procedure for reporting deviations from the direct debit scheme rules;*

– *relevant clauses in contracts with PSPs;*

– *audits and issued recommendations.*

5 THE DIRECT DEBIT SCHEME SHOULD MANAGE AND CONTAIN FINANCIAL RISKS IN RELATION TO THE CLEARING AND SETTLEMENT PROCESS

5.1 THE DIRECT DEBIT SCHEME SHOULD IDENTIFY THE FINANCIAL RISKS INVOLVED IN THE CLEARING AND SETTLEMENT ARRANGEMENTS AND 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 direct debit scheme;*

  – *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.

  Background documents and information:

  – *settlement arrangements used in the direct debit scheme;*

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

5.1.3 FINANCIAL RISK OF CLEARING ARRANGEMENTS

Does the GA evaluate the financial risks arising from the different clearing arrangements and clearing agents used within the scheme? Does the GA mitigate financial risks exceeding 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. This should include financial risks related to the default, insolvency or technical breakdown of a clearing agent and should take into consideration whether or not these clearing agents are engaged in other activities 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 direct debit scheme 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 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 scheme;*

  – *selection procedure and criteria for clearing agents;*

  – *direct debit scheme's financial risk analysis and management report;*

  – *direct debit scheme's financial risk mitigation policies and measures;*

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

5.1.4 FINANCIAL RISK OF SETTLEMENT ARRANGEMENTS

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

technical breakdown of a 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 direct debit scheme 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 scheme;*

  – *selection procedure and criteria for settlement agents;*

  – *direct debit scheme's financial risk analysis and management report;*

  – *direct debit scheme's financial risk mitigation policies and measures;*

  – *direct debit scheme's 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 direct debit 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 the creditworthiness of settlement agents and takes action based on the results of this monitoring.
- The GA monitors the operational reliability (including security risks) of settlement agents and takes action based on the results of this monitoring.
- The GA requires scheme participants to conduct such monitoring.

  Background documents and information:

  – *analysis of the financial, operational and security risks of direct debit settlement agents;*

  – *scheme rules and proof of the monitoring.*

5.2 THE DIRECT DEBIT SCHEME SHOULD ENSURE THAT ALL SELECTED CLEARING AND/OR SETTLEMENT PROVIDERS ARE OF SUFFICIENT CREDITWORTHINESS, OPERATIONAL RELIABILITY AND SECURITY FOR THEIR PURPOSES.

5.2.1 SELECTION PROCEDURE

Does the GA have a procedure to select clearing and/or settlement providers, or are there minimum requirements in place with which clearing and/or settlement agents must comply when accepting clearing and/or settlement providers?

- There is a procedure within the GA to select clearing and/or settlement providers, or there are minimum requirements for clearing and/or settlement agents to accept such providers.

  Background documents and information:

  – *Selection procedure for clearing and settlement providers.*

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

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

- 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 (including security risks) 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.

  Background documents and information:

  – *Analysis of the financial, operational and security risks of direct debit schemes of major clearing and settlement providers.*

5.3 IF THERE ARE ARRANGEMENTS TO COMPLETE SETTLEMENT IN THE EVENT OF AN ACTOR 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 DIRECT DEBIT 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 A SETTLEMENT PROVIDER(S) DEFAULTING

Where arrangements are made to complete settlement in the event of a settlement provider(s) 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.)

- There is a process in place to determine the resources needed, in principle, to complete settlement and to review this on a regular/event-driven basis.

- There is a procedure in place to make the necessary resources available to complete settlement and to ensure that these resources are sufficiently liquid.

  Background documents and information:

  – *direct debit scheme'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?);*

  – *direct debit scheme's default policies and procedures (how will the resources be used in the event 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 the settlement arrangement are aware of their obligations and comply with the relevant regulations regarding solvency?

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

- There is a procedure in place to ensure that settlement providers are aware of their obligations and the potential size of such obligations to complete settlement in the event of another settlement provider 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:

  – *Direct debit scheme'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
Access phase	Phase that encompasses the access of the actors (service providers or customers) to the scheme.
Actors	The actors of the direct debit scheme are the governance authority, the payer's payment service provider (PSP), the payee's PSP, the technical service provider, the clearing provider and the settlement provider, and the customers (payee and payer).
Authentication	A procedure that allows the PSP to verify a customer's identity.
Authorisation	A procedure that checks whether a customer or PSP has the right to perform a certain action, e.g. the right to transfer funds, or to have access to sensitive data.
Clearing agent (operator of the clearing system)	The clearing agent is the operator of the clearing system (e.g. EBA Clearing is the operator of STEP2).
Clearing arrangement	A clearing arrangement consists of a clearing system, as well as any contracts between direct debit scheme actors regarding the clearing of direct debit 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 for other market participants (e.g. a PSP having direct access to a clearing system such as STEP2).
Collection	The process by which the payment service providers transfer funds from the payer to the payee.
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).
Customers	The parties (the payee and the payer) using the services of the direct debit scheme.
Direct debit	A payment service for debiting a payer's payment account, whereby a payment transaction is initiated by the payee on the basis of the payer's consent.
Direct debit scheme	A set of functions, procedures, arrangements, rules and devices that enable the authorised debiting of the payer's payment account initiated by the payee either as a single payment or a series of payments. The oversight framework covers the entire payment cycle, i.e. access to the scheme, the initiation phase, the transaction phase and the clearing and settlement phase. It takes into account concerns relating to both the retail payment system and the payment instrument used.
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 direct debit scheme, 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.

Term	Definition
Financial risk	A term covering a range of risks incurred in financial transactions (e.g. liquidity and credit risks).
Initiation phase	The initiation phase encompasses the creation, management and end (cancellation) of the mandate.
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.
Mandate	The authorisation (consent) given by the payer to the payee and/or to its own payment service provider to debit the account. A mandate may exist as a paper document that has been physically signed by the payer. Alternatively, it may be an electronic document which is created and signed in a secure electronic manner. The mandate, whether in paper or electronic form, must contain the necessary legal text and the names of the parties signing it. In some national variants of direct debit schemes (e.g. one-off direct debit transactions), the mandate is not used.
Outsourcing	Outsourcing occurs when a service provider contracts a third party to fulfil its own responsibilities as defined by the credit transfer scheme. 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.
Payee (or creditor)	A natural or legal person who is the intended recipient of funds in a direct debit transaction.
Payee's (creditor's) payment service provider	The PSP where the payee's payment account is held and which has concluded an agreement with the payee about the rules and conditions of a product based on the scheme. On the basis of this agreement, it receives and executes instructions from the payee to initiate the direct debit transaction by forwarding the collection to the payer's PSP.
Payer (or debtor)	A natural or legal person who holds a payment account and authorises a direct debit transaction from the payment account.
Payer's (debtor's) payment service provider	The PSP where the payment account to be debited is held and which has concluded an agreement with the payer about the rules and conditions of a product based on the scheme. On the basis of this agreement, it executes each collection of the direct debit originated by the payee by debiting the payer's account.
Payment account	An account which is used for the execution of payment transactions.
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 direct debit schemes. Thus, with regard to the compliance with the oversight standards, there is no differentiation between the legal status of PSPs.
R-transactions	The umbrella term for the following terms: • Refunds are claims by the payer for reimbursement of contested debits on the account. • Refusals are instructions issued by the payer prior to settlement, for whatever reason, to the effect that the payer's PSP should not make a direct debit payment. • Reject is the result of a failed transaction whereby the payment has already been declined prior to interbank settlement. Possible causes include technical reasons, a closed account and insufficient funds. • Returns are direct debit collections that are diverted from normal execution following interbank settlement and are initiated by the payer's PSP. • Reversal is initiated by the payee after settlement in the event that a direct debit that has already been paid should not have been processed. Consequently, it is the reimbursement of funds by the payee to the payer. • Revocation is the request by the payee to recall the direct debit collection prior to acceptance by the payee's PSP.
Scheme	Refers to the direct debit scheme.
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 or 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 methods used.
Service providers	Service providers encompass PSPs, technical service providers offering technical services within the scheme (e.g. communications network service, IT service), the clearing provider and the settlement provider.
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 direct debit scheme actors regarding the settlement of direct debit 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 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 (i.e. PSPs).
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.
Technical service providers	Providers that offer technical services within the scheme, such as the communications network service, IT service or other technical services.
Transaction phase	The transaction phase is the whole process of the execution of a direct debit, starting from the collection initiated by the payee up to its finality (the normal execution, or the reject, return or refund of the collection). It is the end-to-end execution of a direct debit payment.
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.