



AFEP Safeguarding Webinar

“Coronavirus and safeguarding customers’ funds: additional guidance for payment and e-money firms”

11 November 2020



**MAKING AN
IMPACT THAT
MATTERS**
since 1845

Deloitte speakers



Dennis Cheng
Director

Dennis has over 14+ years experience advising clients in the banking, capital markets and the wealth management industry. He leads the safeguarding team within Deloitte's Audit and Assurance division in London and currently sits within the ICAEW's Safeguarding Working Group which is due to implement the new Safeguarding Audit requirements as proposed by the FCA's recent guidance.

dencheng@deloitte.co.uk | +44 20 7303 6970



Philip Ackroyd
Manager

Phil specialises in the compliance of e-money and payment services firms, having joined Deloitte last year from the Payments Supervision Department at the FCA. Since then he has focused primarily on firms' measures for safeguarding user funds, helping clients design their approach and carrying out outsourced internal audit reviews in this area. More broadly, he has cross-sector expertise in the evaluation of senior management, governance arrangements and risk frameworks in financial institutions.

packroyd@deloitte.co.uk









Joseph Wood
Senior Manager

Joe is a Senior Manager in Deloitte's Banking and Capital Markets team in London. Having worked in both consultancy and audit disciplines since 2010 he has experience working with a wide range of firms from global investment banks to a small wealth management and payment services firms. He has led safeguarding health checks as well as outsourced internal audit reviews of safeguarding arrangements.

josephwood@deloitte.co.uk

Agenda

	1. Overview of the regulations	4
	2. Operationalising the requirements – the FCA's expectations	6
	3. Building an operating and oversight framework	9
	4. Completing a health check of your arrangements	11
	5. Preparing for the upcoming audits	13
	6. Q&A	20



Overview of the regulations



Overview of the segregation rules in the PSRs and EMRs

The regulatory obligations are covered in relatively short sections of statute.

Defining Relevant Funds

- Under the PSRs 2017, relevant funds are sums received from, or for the benefit of, a payment service user for the execution of a payment transaction;
- Under the EMRs 2011, relevant funds are those that have been received in exchange for e-money that has been issued.

What are the segregation requirements?

Applicable to all APIs and EMIs		Specific to E-Money Institutions	
Reg.	An account in which relevant funds or relevant assets are placed at the end of the business day following the day on which they were received must —	Reg.	Funds received in the form of payment by payment instrument need not be safeguarded until they—
23(7) 21(3)	(a) be designated in such a way as to show that it is an account which is held for the purpose of safeguarding relevant funds or relevant assets in accordance with this regulation; and	20 (4)	(a) are credited to the electronic money institution's payment account; or
	(b) be used only for holding those funds or assets.		(b) are otherwise made available to the electronic money institution, provided that such funds must be safeguarded by the end of five business days after the date on which the electronic money has been issued.
23(8/23) 22(2)	No person other than the authorised institution may have any interest in or right over the relevant funds or relevant assets placed in a safeguarding account.		
23(11) 21(5)	The authorised institution must keep a record of any relevant funds segregated and any relevant funds or assets placed in a safeguarding account.	20 (6)	Regulation 23 of the Payment Services Regulations 2017 applies in relation to funds received by electronic money institutions for the execution of payment transactions that are not related to the issuance of electronic money.
23(17) 24(3)	An institution must maintain organisational arrangements sufficient to minimise the risk of the loss or diminution of relevant funds or relevant assets through fraud, misuse, negligence or poor administration.		
		<div>Legend: Payment Services Regulations 2017 (reg.23) E-Money Regulations (regs. 20-22)</div>	

What are the Control Requirements?



Firms must ensure the sound and prudent conduct of the affairs of the institution through:

- robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility;*
- effective procedures to identify, manage, monitor and report any risks to which it might be exposed; and*
- adequate internal control mechanisms, including sound administrative, risk management and accounting procedures.*

PSRs 6 (6)
EMRs 6 (5)

Operationalising the requirements – the FCA's expectations



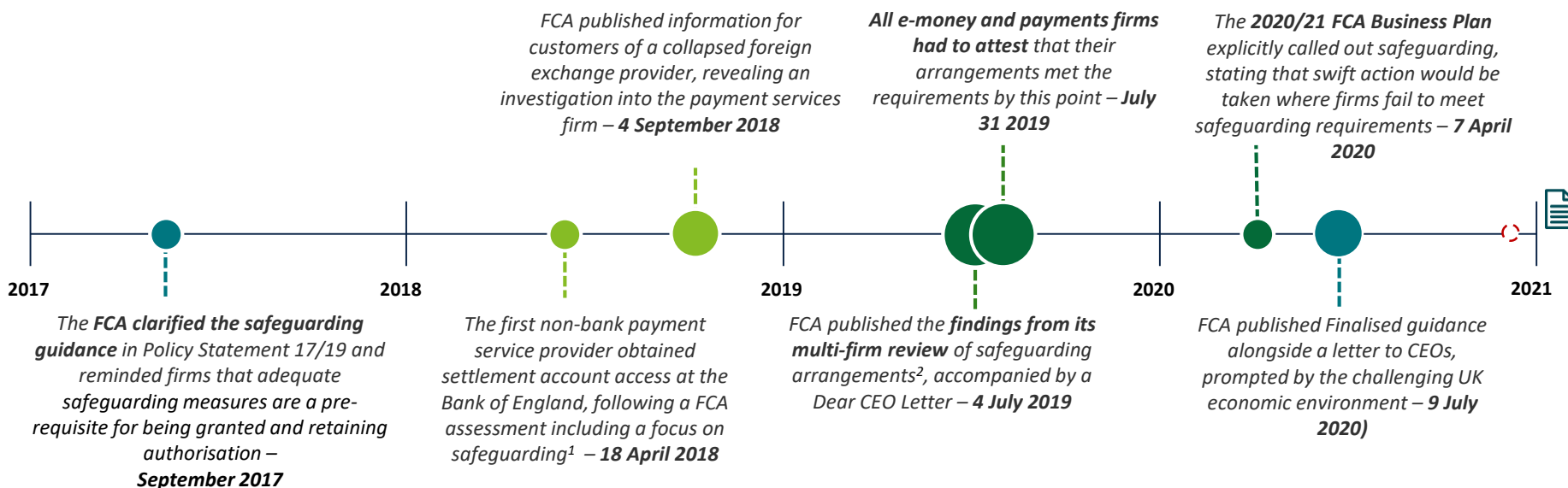
The FCA published its Finalised additional guidance in July 2020

Following the Dear CEO Letter and attestation process last year, the FCA has issued further guidance in light of the ongoing COVID-19 crisis – underlining safeguarding as a supervisory priority.

Regulatory Focus

The regulator is concerned that safeguarding shortcomings would hinder the repayment of outstanding customer claims should one or more payment services or e-money firms fail. The guidance should help firms prevent harm to their customers in such an event, by making the wind-down process as orderly as possible and protecting them from financial loss or other detriment.

Timeline



Legend:

- Policy Development
- Market Event
- Supervisory Action



The FCA plans to publish a consultation on its Approach Document to incorporate recent guidance – Q1 2021

¹ <https://www.bankofengland.co.uk/-/media/boe/files/markets/other-market-operations/accessfornonbankpaymentsserviceproviders>

² <https://www.fca.org.uk/news/statements/information-customers-premier-fx-limited>

The FCA's expectations for operationalising the requirements

In its Approach Document and Finalised Guidance, the FCA sets out its view on how fees and other sources of funds sitting within a segregated or safeguarding account should be protected in practice.



Identification of relevant funds

- Firms often receive relevant funds from customers bundled with other non-relevant sources. They may also earn the right to deduct fees/ other charges, as part of the transaction lifecycle.

- They must distinguish between funds received for the execution of payment transactions and those held for other purposes to determine the correct amount of relevant funds.
- The firm's relevant funds footprint will depend on its business model and the services offered.



Safeguarding of funds

- Firms must safeguard funds as soon as they are received by either the segregation method or the insurance/ comparable guarantee method. An institution may use a combination of these.

- If using the segregation method, relevant funds continuing to be held at the end of the business day following the day of receipt must be deposited in a protected safeguarding account held with an authorised credit institution (or the Bank of England).



Avoidance of co-mingling

- Co-mingling, even for short periods, increases the risk of corrupting the pool of funds that would pay the priority claims of payment users/ e-money holders in case of firm failure.

- Firms using the segregation method must hold funds in a separate account from their own working capital.
- Firms must remove other sources of funds from segregated accounts as frequently as practicable throughout the day.
- Other sources of funds include transaction fees, and security payments/ margin on FX transactions.



Reconciliations & record keeping

- Firms must carry out reconciliations to ensure the correct amount has been safeguarded.
- Excessive or insufficient balances should be rectified.

- PSPs also need to maintain records that are sufficient to identify the individual entitlement of users to the funds and, if applicable, evidence what funds have been separated and how.
- Firms should carry out reconciliations as often as necessary to manage the risk of discrepancies and have well-designed controls to check their completeness.



Account administration & protections

- Safeguarding accounts require heightened protections compared to accounts opened under standard terms.
- The FCA considers that a firm holds funds on trust for its customers.

- They must be designated as either "safeguarding", "client" or "customer" accounts and there should be clear evidence - in the form of a letter - that no-one other than the payment service provider has an interest in or right over the funds in the accounts.



Also applicable to Guarantee Method

Other **governance and control activities** expected by the FCA include:

- the appointment of a suitable individual to oversee compliance with the regulations;
- appropriate due diligence over safeguarding third parties;
- documenting the rationale** for every decision made regarding the safeguarding process and the systems and controls in place.

[Source: Approach Document, paragraph 10.59]

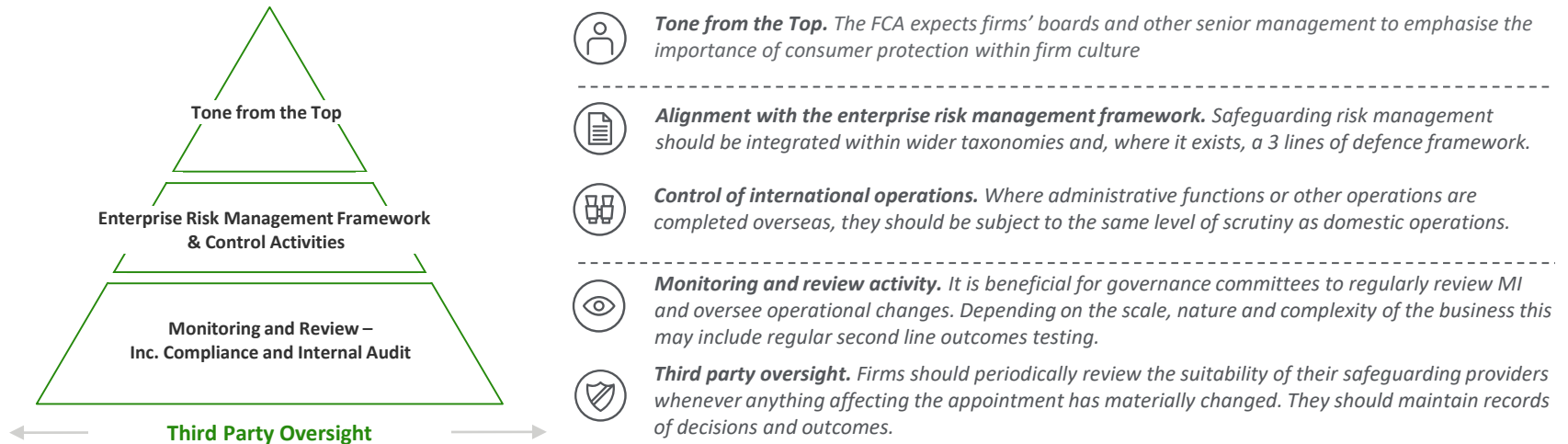
Building an operating and oversight framework



Building a safeguarding operating and oversight framework

A well-designed approach is important for effectively managing risks to the integrity of relevant funds.

Framework Structure



Good Governance in Practice

Governance describes the **procedures used in the decision-making and control** of the business that provide its **structure, direction and accountability**. The FCA recently identified inadequate governance and oversight as a root cause of regulatory issues. The following principles in this area are key to well-organised safeguarding arrangements:

- **Formalise executive ownership of risks** and responsibilities for safeguarding compliance. These should be represented through **clear organisational structure charts and coverage in the terms of reference** across all relevant committees;
- Ensure senior management have **specific knowledge and experience** of how regulatory processes are implemented and **conduct regular reviews of the firm’s safeguarding policies and procedures** so that they remain suitable even as the firm’s business and operating model changes. Decisions should be recorded;
- Where the firm is part of a multi-national group, **maintain decision-making authority in the UK business** and ensure there is a framework in place for **escalating important matters to the Board** from across the entirety of the firm’s relevant operations.

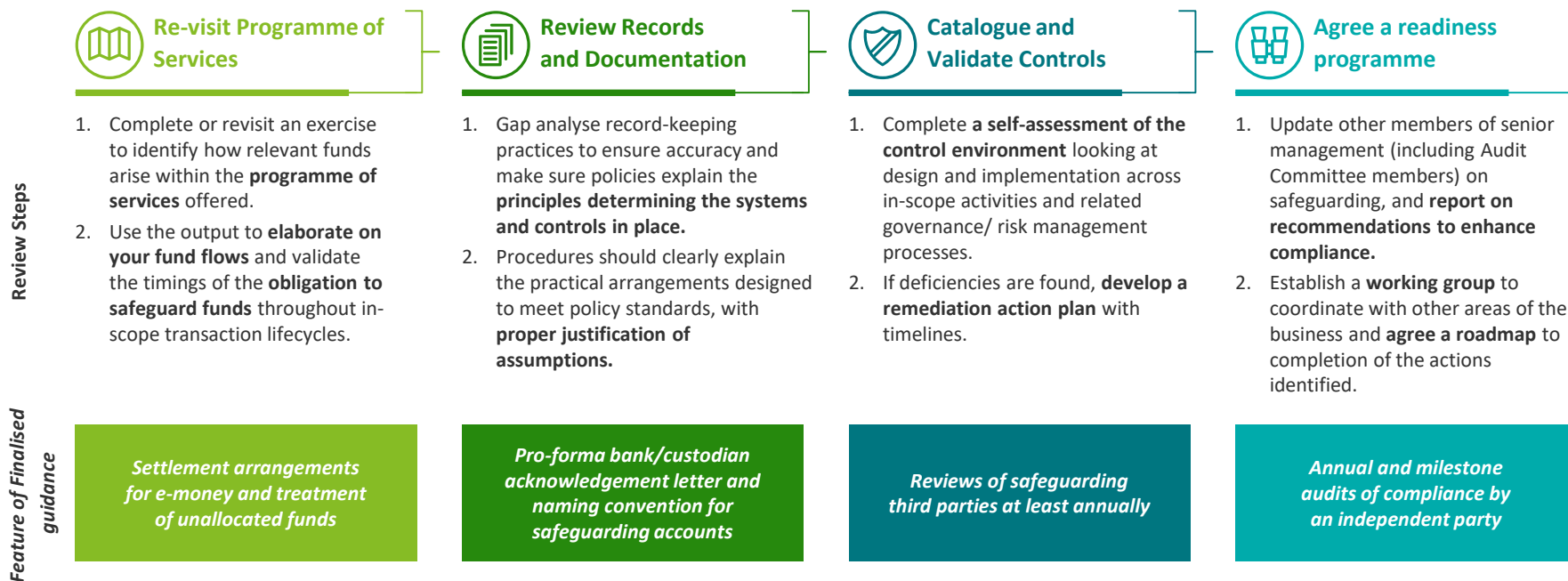
Completing a health check of your arrangements



Implementing the Finalised guidance and acting on the Dear CEO Letter

Firms will benefit from a proactive approach to discussing the new guidance at a senior level, carrying out review activity and taking remedial measures where necessary.

The senior individual with overall responsibility for safeguarding compliance may wish to undertake a **readiness review of the firm's organisational arrangements**. Typically, this will involve a **mapping exercise** to analyse whether the firm's operating systems are comprehensive in meeting the regulator's expectations for managing firm-specific risks to relevant funds and **re-evaluate whether the controls and management information** in place give comfort that they are functioning properly.



Safeguarding Policy – Documenting your rationale

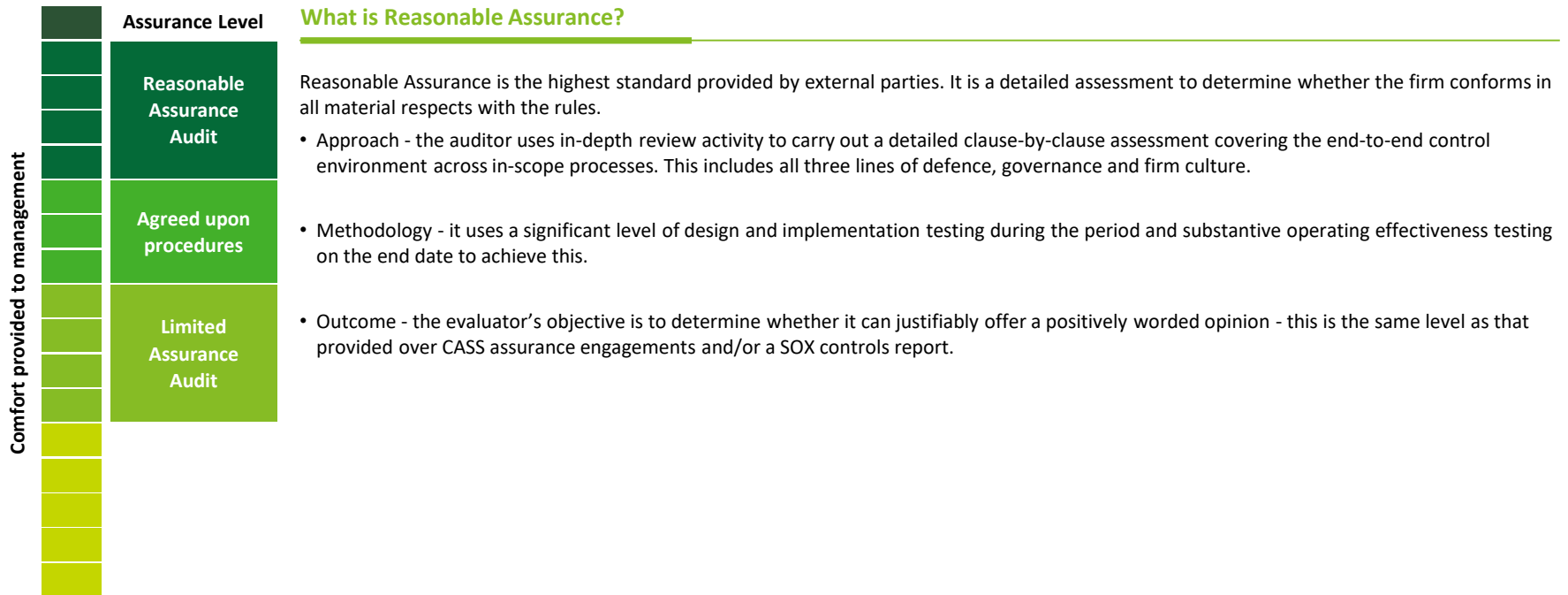
Firms' rationale for the systems and controls in place should be **detailed enough to convincingly explain** to key independent stakeholders **why the firm has decided to take such an approach**. To achieve this, the firm's policy will need to clarify the **firm's interpretation of the regulations that apply** to its payment service activities.

Preparing for the upcoming audits



Building a fourth line of defence: External safeguarding audits

The FCA Finalised Guidance has outlined that firms need to obtain an annual reasonable assurance opinion in regards to their compliance with the safeguarding requirements and expectations in the EMRs and PSRs as well as the FCA Approach Document.



In addition the regulator expects firms to arrange interim audits should significant changes to the business model take place that materially affect safeguarding arrangements.

What type of audit is required?

The FCA defined the key characteristics of the opinion in paragraph 1.20 of their latest guidance. In lieu of a specific auditing standard for these engagements, the ISAE 3000 framework is likely to be adopted across the industry.

Finalised guidance

Coronavirus and safeguarding customers' funds: additional guidance for payment and e-money firms

9 July 2020

1.20 We expect the auditor to provide an opinion addressed to the firm on:

- whether the firm has maintained organisational arrangements adequate to enable it to meet the FCA's expectations of its compliance with the safeguarding provisions of the EMRs/PSRs (as set out in chapter 10 of our Approach Document), throughout the audit period, and
- whether the firm met those expectations as at the audit period end date.

Areas for clarification

- What does "meet the FCA's expectations" mean?
- There is a possibility of further guidance being published ahead of the already flagged industry consultation scheduled for Q1 2021

1

Stipulates the requirement for a controls approach to be taken for the 'during the year' audit work

2

Period end compliance / substantive testing will be required to assess compliance

How are your key controls documented?

Firms need to have a **control inventory** which clearly articulates the control activities they operate to ensure the requirements of the regulations and associated FCA approach documentation are met.

Features of a control

- When documenting / designing controls thought needs to be given to the nature, approach and type of the control best suited to address the risk.

More reliable		Less reliable	
Preventive		Detective	
Automated		Manual	

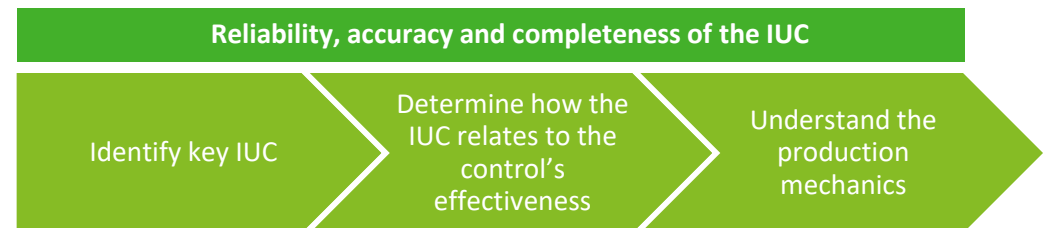
Controls ≠ Processes

- Care needs to be taken to flag and document controls rather than processes. Also considering what evidence needs to be maintained to document and evidence operation of the control.
- Words such as; “post”, “prepare”, “document”, “determine”, “calculate” are indicative of processes. Whereas words such as “review”, “assess”, “approve”, “reconcile” tend to relate to controls

Typical types of controls	
Authorizations and Approvals	Physical Controls and Counts
Verifications	Reconciliations

Information Used in a Control, “IUC”

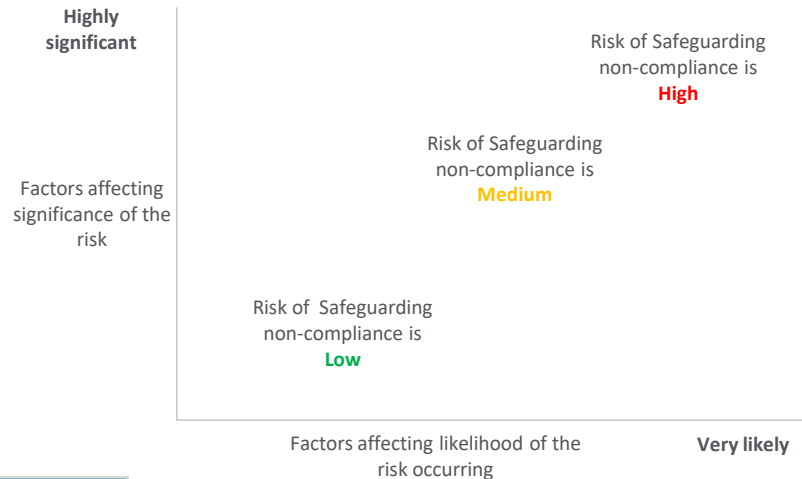
- When automatically generated reports are used a consideration must be given to how the completeness and accuracy of the data within the report is verified.



Moving towards a complete risk applicability and controls matrix

Our expectations for supervision of the non-bank payment services industry would appear to be broadly following the path taken by the regulator in its oversight of investment firms and banking entities.

- Firms should also consider developing a **Safeguarding Rules-to-Risk-to Control mapping** or risk applicability matrix.
- This “live document” if done well becomes a powerful tool to demonstrate to regulators, auditors and in house stakeholders that the firm has appropriate safeguarding risk identification, management and mitigating controls in place.
- With the inclusion of control attestations and / or monitoring by 2nd / 3rd line of defence, such tools can also be used by firms to identify risk hot spots, and areas of focus.



Firm's risk assessment	Risk of non-compliance with the Safeguarding requirements			Actions taken by firm
Safeguarding Risk 1 – e.g. identification of funds	H			E.g. Mitigate with Control X
Safeguarding Risk 2 – e.g. reconciliation discrepancies		M		E.g. Mitigate with Control Y
Safeguarding Risk N			L	E.g. Mitigate with Control Z

What will a controls based audit look and feel like?

When assessing a control both the “design and implementation” of each key control needs to be evaluated. Should these factors be deemed appropriate “operating effectiveness testing” over the ‘audit period’ will be executed. Where relevant IT testing will also be completed.

Key design factors of a control

Appropriateness of purpose of control and its correlation to risk

Competence and authority of person(s) performing control

Frequency and consistency with which control is performed

Level of aggregation and predictability

Criteria for investigation and process for follow-up

Assessing implementation

Inquiry

Observation

Inspection

Trace transactions / information through the
process & control

Q&A





This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please [click here](#) to learn more about our global network of member firms.

© 2020 Deloitte LLP. All rights reserved.

Designed by CoRe Creative Services. RITM0510913