Good Practice Guidance for Member Firms

Topic: Risk Management Guidance

Date published: May 2020

Next Review Date: May 2021

1. About AFEP

Founded in 2012, AFEP works on behalf of its members to be the representative body for Authorised Payment and Electronic Money Institutions. Our mission is to elevate the standards of the FX and e-money industry, and advocate on behalf of our members with regulators and government bodies.

2. Background

In June 2019 the FCA published version 4 of its role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011 (Payment Services and Electronic Money – Our Approach). The whole document is in fact "their approach" or more specifically, "their expectations" of how a firm should manage its *risks*[1].

Risk management is a diverse subject and AFEP have published several good practice guidelines that relate to specific risk management disciplines such as corporate governance, anti-money laundering and safeguarding. The intention of these guidelines is to provide our member firms with a proposal for taking a more holistic, or entreprise wide approach to risk management and in so doing be better prepared for regulatory requests for information relating to thematic reviews, diagnostic visits or other such external requests that present a firm with the opportunity to explain how risk management is at the forefront of their day-to-day business activities and new business pipeline.

Members that also have an investment firm as part of their group will be used to discussing and documenting its risk management framework when going through their internal capital adequacy assessment process (or "ICAAP"). Increasing we are seeing the FCA request similar information from Payment and e-Money institutions. We believe that the FCA will, with increasing frequency, ask member firms for information that is more investment firm like, and potentially in the future consult on requirements that may in the future apply to Payments and e-Money institutions. These requirements may look much more like those that relate to an ICAAP and the Supervisory Review and Evaluation Process ("SREP") outlined in IFRPRU 2.2

In November 2019 we saw the EBA publish it finalised guidelines, EBA final guidelines on ICT and security risk management, and in December the FCA published CP 19/32[2] - Building operational resilience: impact tolerances for important business services and we noted that the FCA took the opportunity to emphasise that all FSMA firms "…and firms providing payment services or e-money services, are subject to the Principles for Businesses (PRIN)." Which includes statements as to maintaining adequate financial resources, and the assessment of appropriate resources under the threshold conditions there is an expectation that the firm will take reasonable steps to identify and measure its risks.

Looking ahead, we see more investment firm like regulation being applied to this sector and we are publishing this guidance so that members have an opportunity to pro-actively consider what proportionate steps can be taken to strengthen their risk management practices and better evidence these practices their Boards and regulators.

[1] This guidance has been put together considering section 3 - governance arrangements, internal controls and risk management (regulation 6(6) *and* paragraphs 5 to 11, Schedule 2 of the PSRs 2017 and regulation 6(5) and paragraphs 5 to 6 Schedule 1 of the EMRs)

[2] The FCA published a Consultation Paper in December 2019 (CP 19/32 - Building operational resilience: impact tolerances for important business services) which we are responding to as a separate piece of work during September 2020.

3. Glossary of key terms

Term	Definition	Abbreviation
Entreprise risk management framework	A documented framework that incorporates *all* risks that a member firm is exposed to in order to deliver its business objectives and one that measures and reports exposures to these risks in an objective way to the Board and shareholders.	ERMF
Controls Library	A list of the controls that are in place to minimise the likelihood and/or impact of a risk event that leads to a direct or indirect financial loss.	-
Direct financial loss	An actual financial loss resulting from a risk event	
Indirect financial loss	A loss or unexpected cost that that has yet to materialise as a result of a risk event	
Inherent risk	A risk that is present when undertaking a business activity (e.g. IT security risks are inherent as a result of using connected networks to communicate). An inherent risk *assessment* is an attempt to quantify the risk in the absence of a control.	-
Line of business	Any area in a firm that is not 2LOD or 1LOD	LOB
Line of defense	Group of individuals that responsible for managing, controlling and reporting risk. 1st line of defense - the business owners, whose role is to identify risk, as well as execute actions to manage and control it 2nd line of defense – control functions such as risk, compliance, legal and sometimes finance who are responsible for establishing policies and procedures and serving as the management oversight over the 1LOD 3rd line of defense – groups of individuals that report independently to the board or the audit committee and include functions such as internal audit, external auditors. These groups are primarily involved in controls testing and other assurance activities	LOD 1LOD 2LOD 3LOD
Residual risk	The risk that is present after controls have been applied; or the risk that credit mitigation techniques are as effective as expected (e.g. margin calls not being met). A residual risk *assessment* is an attempt to quantify the risk after the controls have been put in place.	-
Risk Control Self-Assessment		RCSA
Risk Register	A list of all the risks that a member firm is exposed to and the description of what this risk means. Its purpose to remove subjectivity from risk categorisation.	-
Risk Event	A risk event is any event that was an unexpected outcome. An internal risk event is an unexpected outcome that has its origin or impact inside the firm	IRE

Term	Definition	Abbreviation
	An external risk event is one that has both its origin and impact outside the firm.	ERE
Scenario analysis	The use of hypothetical situations to understand where there could be gaps in the control framework and take action pro-actively to avoid such situations resulting in a direct or indirect financial loss	
Stress testing	Taking real situations and/or processes and subjecting them to increased load. Taking one or both sides of a matched principal position and applying a severe adverse scenario and analysing the results.	

Note that scenario analysis and stress testing are best applied in combination to demonstrate the interconnected nature of risks and therefore the holistic approach needed to design and monitor controls.

4. Introduction

As the industry and our member firms mature, and AFEP see regulatory requirements, previously reserved for Banks and Investment Firms, attach to Authorised Payments and Electronic Money Institutions, AFEP believe it is prudent to publish some more general good practice guidance for Risk Management in the broader sense of the phrase, and ask members to consider our examples of good and poor practice with a view to implementing more robust risk management practices that will ultimately lead to better information and better evidence to support the business decision making processes.

AFEP recognises the importance of members not only adhering to the FCA rules, but also these Good Practice Guidance documents. Member firms are required, as a condition of membership, to confirm they are using the Good Practice Guidance and applying it to their business to ensure that they can evidence a standard of risk management that is beyond the basic minimum requirements.

Notwithstanding compliance with regulation, AFEP realises that if member firms set out on a risk management journey where the goal is simply to comply with regulations it is likely to become a so-called "box ticking" exercise. AFEP does not advocate this approach, and has written this Risk Management Guidance in such a way the business value can be achieved, problems avoided and the costs of operational losses and the impact of unexpected costs driven down so that for the same revenue, profitability can be increased.

Good Practice Guidance documents have been written and issued to members on the following topics:

1. Communications with customers (currency convertors & disclosure)
2. Safeguarding
3. Customer interests & Conflicts of interest
4. AML
5. Corporate Governance

All five are specific risk management disciplines, and AFEP is looking to highlight (in this document) as to how risk management, like compliance, is not something that the Risk or Compliance teams are solely responsible for. As a second line function these teams have specific responsibilities for setting out the frameworks, and in certain cases performing the tasks associated with the monitoring. It is for the first line (the business areas) to adopt these practices, sponsored by the senior management team and Board, and cascaded throughout the firm by the middle managers who ultimately are closest to the day-to-day activities and responsible for setting the day-to-day priorities.

4.1. What is risk management?

The ISO definition of risk is "the effect of uncertainty on objectives"; the ISO definition of risk management is "coordinated activities to direct and control an organization with regard to risk" [ISO 31000:2018]

With these definitions in mind it is easy to see how the subject is simply too broad for the risk or compliance team to be responsible for all risk management activities. The first recommendation in this good practice guidance is allocate responsibilities clearly and hold the right people responsible for the risk management activity that is in the spotlight.

4.2. Current landscape for risk management

Whilst there is a substantial amount of regulation, guidance and commentary on the topic of risk management. Different rules apply to different types of firm and at times it may be difficult to navigate because, unlike specific

risk management disciplines (such as anti-money laundering), a more general approach to risk management is not something that the regulations or underlying legislation defines specifically.

Moreover, it has often been the case that more specific regulations only arise as a result of specific issues that have both manifested themselves and, where the existing regulations or underlying legislation was not specific enough and therefore frustrated a national competent authority investigation after the fact.[3]

This is one reason why a minimum requirements approach is unlikely to work at any firm. How will a firm know when it has fallen below minimum requirements, and how can it predict which rules will be made more specific next? Firms should implement a risk management framework that is proportionate and a scalable for their business model, instead of attempting to navigate or replicate a regulatory framework for risk management and deliver the minimum requirements.

Notwithstanding the business benefits of a robust and well documented risk management framework AFEP are seeing the FCA request the following from member firms on a more frequent basis.

- Most recent management information (for example monthly or quarterly pack and the minutes from the meeting) submitted to the management body (i.e. Board Committees, Executive Committees or others as applicable),
- Details of the firm's [entreprise] risk management framework and how it fits within the wider group framework,
- Details of the firm's risk governance, oversight and control arrangements (should include details regarding roles and responsibilities, policies, procedures, among others) and how they fit in the wider framework,
- Details of the firm's overall risk appetite and sub-components and how they fit within the group framework, and
- A list of all [risk events] incidents over the past 12 months, in an excel format, including material, non-material and near misses and associated root causes.

AFEP believes that these more recent requests for information by the FCA of member firms are indicative of a pro-active approach from FCA in the sector and the publication of these good practice guidelines is timely, giving our member firms the opportunity to implement good practices and provide a good account of themselves to FCA amongst other independent parties such as Board members and external auditors.

[3] The Senior Managers and Certification Regime ("SMCR") is a good example of existing regulations being strengthened and made much more specific as a direct result of wide-spread issues in the financial services industry. It has always been the case that firms were required to organise themselves effectively and apportion responsibilities to its senior management (SYSC 2.1), and delegate appropriately (SYSC 3.2.3.) SMCR raising the bar significantly and assigning prescribed responsibilities to individual senior managers in an effort to untangle complex and/or undocumented responsibilities which could serve to frustrate successful enforcement action against alleged recidivist individuals.

4.3. Key benefits of implementing an entreprise wide risk management framework

The key benefit and overarching business reason for implementing an entreprise risk management framework ("ERMF") is to protect revenue and maintain profitability.

An ERMF, in a mature state, allows the Board and senior management to identify and prioritise their highest risk activities and direct human and technology resources towards these risks by using data that has its origin within the firm (i.e. is both relevant to the firm, and in the context of other matters at that firm).

This is information can therefore be used to drive down both the likelihood and impact of operational losses, unexpected costs and in so doing, for the same revenue, increase profitability in the medium to long term.

Rather than simply looking at operational losses (actual losses, a direct financial impact), an ERMF looks at the potential for losses as a result of an event, or combination of events and can support the Board and senior management to consider and assess the indirect financial impact too (i.e. the loss or unexpected cost that has not yet materialised, but may do so in the future).

Whilst this document will consider the impact and potential consequence of risk management failures at the end of this guidance AFEP believes that an ERMF has is more likely to gain momentum within in a firm and deliver the expected benefits if, from the point at which the ERMF is conceived the focus is on the benefits of implementing it rather than the consequences of not doing it.

5. Key components of a risk management framework

A risk management program needs be proportionate to the scale and complexity each firm, and firms will need to decide how to right-size the framework for their specific business needs. All firms will however need to have at least the following in place.

Governance: documented governance arrangements that evidence risks are being considered, controlled and that the firm has set out their appetite for certain types of risk.

Tools: risk assessment tools to identify and measure risk, and to ensure that the actions arising from these risk assessments are owned and progress tracked, and policies to ensure employees have boundaries within which to work.

Use Test: The process by which a firm demonstrates effective risk-based capital management, strategic risk management and decision-making.

The following sections will discuss each component in more detail, provide examples of good and poor practices so that AFEP members can assess themselves against each category and decide what if any changes are necessary to achieve their target maturity level.

When AFEP considers scale and complexity, it considers not only the size of a firm or the complexity of the products it offers, but also (and more importantly) the scalability and complexity of the underlying processes that are currently being used to support the business activities.

5.1. Governance

Governance in this context is how the firm's governing body demonstrate and evidence that they have taken all reasonable steps to ensure the risks that are inherent in their business have been identified, measured and are being controlled within the boundaries set by Board, (i.e. the Board stated Risk Appetite).

5.1.1. Identifying risks | Risk Register

Firms should attempt to remove subjectivity from risk identification processes and create a "risk register", a list of risks the meanings of which are well understood. There should also be traceability between generally accepted industry terms and/or regulatory definitions such as those that can be implied from Article 324 of the Capital Requirements Regulation for operational risk.

- Firms should create at least one additional level of specific risk below each of these categories and define some examples of the activity that might lead to the risk manifesting in the business.

- Firms should consider whether they need additional components of their risk register which are of more importance to their business model for any reason. For example, some firms may choose to have a specific risk register for Information Risks, Financial Crime, or Conduct[4].

- Firms should list their financial risk categories (i.e. market, credit and liquidity risks) and clearly articulate how these risks arise

- Firms should exercise caution when deciding to exclude a risk that is inherent in its business model where it believes that should that risk manifest itself the loss would be covered by insurance

5.1.2. Setting and documenting risk appetite | Risk Appetite and Metrics

The Board is accountable for setting risk appetite and the executive management are responsible for ensuring they remain within stated risk appetite and escalate instances where the firm may be outside (or about to be outside) the stated risk appetite.

A documented statement of risk appetite is not only a regulatory requirement but a good document for the Board to articulate what it expects from its senior management team and other employees. If the document is both qualitative and quantitative, the qualitative statements can be used to frame the sorts of behaviours it expects going some way to defining a firm's code of conduct and culture.

- Firms should have documented statements of risk appetite, and quantitative metrics that measure where the firm is against the stated risk appetite.

- The quantitative metrics used should be reported to the firm's governing body (e.g. Board, Audit and Risk Committee, Executive Committee as appropriate), the metrics should be consistent with the risk appetite statement[5] and instances where the firm is outside of risk appetite must be escalated to the Board.

- Firms should define a risk appetite statement for at least all risk types that it believes are material to its business model and be able to justify its selection.

- Firms should be able to quantitatively assess any risk that it has set a risk appetite for, and should monitor it at a frequency that is commensurate with the specific risk's rate of change (i.e. if the risk profile changes daily it should be measured daily).

- Firms should set quantitative thresholds that are designed to capture high utilisation (AMBER), and at what level they should set them to avoid being surprised by being outside of risk appetite (RED).

[4] AFEP recommends that its members reference an FCA publication further to its review of the wholesale banking supervision, its third report published in May 2019. 'Progress and challenges' 5 Conduct Questions Industry Feedback for 2018/19 Wholesale Banking Supervision. Some of our member firms are captured by SMCR and therefore will have SMF functions and certified individuals responsible for implementing and measuring the outcomes of its conduct risk framework, and for member firms where the SMCR does not apply the messages are relevant to obligations under PRIN, SYSC, and COBS.

[5] If a firm decides that it has zero appetite for any risk, a quantitative assessment greater than zero will be outside of risk appetite and therefore must be reported to the Board.

5.1.3. Documenting senior management responsibilities | Apportionment

As mentioned in the section on current landscape of risk management (section 3.2), the concept of apportionment existing before SMCR, and applies to all member firms whether or not captured by SMCR.

- Firms should document who of the senior management team is responsible for each risk management activity and which of the governance forums that senior manager is accountable to, or responsible for reporting their risk information to.

- Firms should apportion responsibilities to the most appropriate member of senior management team (i.e. to the senior manager who has been appointed and is remunerated on the basis that they understand and are able to articulate the risks they are responsible for; or those risks that are inherent in the business activity they are responsible for).

- Firms should consider the statements they have made as to any "three lines of defense" model and make a clear distinction between first, second and third line of defense[6]. Where responsibilities are shared, articulate and justify the basis on which they are shared.

- Firms should incorporate risk management responsibilities into senior employees' job descriptions, objectives. Their responsibilities should include staying current with regulations that apply to the risks they manage (e.g. COO/C(ISO) is responsible for understanding regulations that relate to operational resilience).

5.1.4. Ensuring policies and procedures are being followed | Policy Assurance

Policies and procedures are fundamental to any risk management framework and we encourage firms to have an appropriate and proportionate amount of policy and procedural documentation. We also encourage firms to ensure their accountable and responsible executives can evidence that they are taking all reasonable steps to ensure their policies are being followed.

- Firms should have a documented approach to policy assurance and a monitoring program

- The monitoring program should not simply be left to the risk, compliance or audit function to operate. The accountable executive for the policy should actively seek out evidence of compliance and non-compliance

- Firms should ensure that policy breaches are treated consistently (i.e. the same response should a policy requirement be breached by a revenue generator or a non-revenue generator)

- Firms should identify areas of known, or planned non-compliance (where a policy is still embedding) and create for formal risk acceptance policy or procedure that takes a risk-based approach and ensures that the right executive accepts the risk[7]

[6] Where a member firm refers to three lines of defense model and purports to have one in place there will be an expectation that the three lines model exists and can be evidenced.

[7] Risk acceptance is often signed-off by the individual responsible for putting the framework in place to manage the risk rather than risk taker themselves. Firms often see this with risk acceptances that relate to IT Security. It is not the role of the C/ISO to accept the risks associated with gaps in the security framework, it is their role to properly understand and articulate them to the CEO, CFO or other senior manager that has responsibility for setting budget and priority to sign-off.

5.1.5. Table 1 – Examples of good and poor risk management governance practices

Examples of good practice	Examples of poor practice
Senior management are seen to actively sponsor the components of the ERMF, and middle management ensure these components are prioritised within the day-to-day activities. This approach increases the probability of the messages from the ERMF embedding in the firm and adding the expected business value.	Risk management is seen as something that one or two individuals in the Compliance department are responsible for. Senior management do not actively sponsor the ERMF and as a result middle management see it as pointless bureaucratic exercise and a roadblock to business agility.
Every attempt is made to remove subjectivity from the risk language and a formal document is created and reviewed by the governing body as to the list of risks that the firm is exposed to and how they might arise. The Risk Register (risk taxonomy, list of risks), is mapped back to industry standard terms and the appropriate regulations.	The risk register is blended with a risk assessment, there is no specificity for the way the firm is organised or the products that it offers, and it has not been updated since either authorisation or reauthorisation.
There are documented statements of risk appetite that have been approved by the Board and traceability between the risk appetite statements and the risks in the risk register. There are metrics in place to quantitatively assess risk profile against risk appetite and thresholds are set as an early warning (high utilisation) so that action can be taken before the firm is outside of risk appetite.	Statements are not documented, or there is no evidence of Board sign-off. The statements themselves are vague (e.g. a low risk appetite for operational losses), and there is limited traceability between risk appetite statements and the risks that the firm purports to be taking.
The risk appetite metrics have been approved by the Board and are collected from a wide source of existing management information (1st and 2nd line), that is being used to make business decisions already. These metrics consolidated so that senior management can see the context of one risk metric versus another. An entreprise approach, a holistic approach, which has also been reviewed and challenged by an individual in a 2nd line function.	The management information being provided to the governing body is not delivered in a way that puts one metric in the context of another. The 2nd line functions are expected to produce all the risk management information and 1st line representatives are not held accountable for explaining the information that is being put in front of the governing body.
Policies, or policy statements within manuals are unambiguous, there is consistency with risk appetite, and traceability to regulatory and legal obligations. There are procedures to support the implementation of the policy or policy statements within manuals. The accountable and responsible executive can evidence that they have taken all reasonable steps to assure their policies and escalated any areas of non-compliance to the appropriate forum, and/or has documented risk acceptances that are specific and timebound.	Policies, or policy statements for regulated activities or the processes that support regulated activities are not documented, signed-off by the firm's governing body, nor is there any evidence that the accountable or responsible executives have made any attempt to assure the policy or policy statement within a manual. Accountable and/or responsible executives rely on a Compliance function explain and provide training on *all* regulatory matters, even those where they are themselves are remunerated as the subject matter expert (e.g. IT Security or Financial Returns).

5.1.6. Indicators that a firms entreprise risk management framework is likely to succeed

Efforts to implement an ERMF must are focussed, resourced appropriately and raised up in the firm so that it is easy to establish their relevance. The near-term result is more likely to be continued momentum rather than "starts and stops" and ceaseless discussions focused on understanding what the objective is. The longer-term result is more likely to be that risk management is elevated to a strategic level and is driven in an entreprise wide way instead of a silo approach.

Common indicators a successful framework include

Organisational indicators:

- Support from executive management and other key stakeholders and traction due to accountability and delegation of the initiative to more senior middle managers in the firm.
- The ERMF initiative is enterprise wide in scope, and strategic in focus.
- The executive management take steps to prevent an "additive" point of view which assumes that the various risk management silos combined will constitute an ERMF response because they collectively cover the enterprise's risks. Instead they actively sponsor a truly entreprise wide approach and ensure that the risk management silos collaborate and communicate to achieve the desired response

Process indicators:

- There is a risk management policy, or a document that described the ERMF principles that is subscribed to by the business and the risk management silos
- The ERMF process focusses on the vital few risks that really matter and/or positions the firm as an early mover to capitalise on market opportunities and emerging risks.

Behavioural indicators:

- There is clarity as to the business motivation and an economic justification for the ERMF, rather than constantly trying to understand "the problem we're trying to solve with ERMF," leading to endless dialogue about the "what" and "why."[8]
- The ERMF starts to respond, in a manner acceptable to the Board, to such questions as: What are our most critical risks? How well are we managing them and how do we know?
- Instead of paralysis (i.e., unwillingness to start somewhere to ensure an effective enterprise wide approach to managing risk), the firm acts and starts with the components of the ERMF that require the larger data sets to succeed (e.g. risk events and loss data which will be described in the next section).

[8] An ERMF does not get implemented because a firm is trying to *solve* a problem, it gets implemented because firms are able to recognise the value and importance of avoiding problems in the first place.

5.2. Tools

The key risk management tools are

i. risk assessments, more specifically, risk and control self-assessments ("RCSA"), and a "Controls Library"

ii. risk event and loss event reporting,

iii. key risk indicators, and performance indicators,

iv. scenario analysis and stress testing, and

v. a policy framework

The next sections describe each in turn.

5.2.1. Risk assessments | RCSA and Controls Library

An RCSA can be performed at business unit or at legal entity level depending on the size of the firm. It should assess the inherent risk (i.e. the likelihood and impact without controls) and the residual risk (i.e. the likelihood and impact after control). The methodology for assessing inherent and residual should consider known events and be signed-off by the business unit manager.

- Firms should have an agreed RSCA template that incorporates both the risks and controls associated with the key activities that could lead to any given risk, and controls should be categorised as preventative or detective

- Controls should be assessed as effective, partially effective, or ineffective as part of the RSCA process and a program of controls testing should be in place for at least the higher risk activities

- Firms should have a defined criterion for likelihood and impact (e.g. if the likelihood is qualitatively assessed as "high", "almost certain" these parameters should be defined in some way). With respect to impact, bands should be established with reference to the firm's appetite for loss[9].

- Authorised Payments Institutions and e-Money Institutions are required to submit an Operational and Security Risk Assessment to FCA on an annual basis (the "REP018)

- Firms should ensure that the individuals with the expertise in the activity participate, contribute to and ultimately own their own RSCA where an RSCA is performed at business unit level (e.g. Operations, Finance or IT), where firms choose to perform an RSCA at legal entity level they should ensure that the document has been thoroughly reviewed by the managers at business unit level

[9] Some firms may have already defined their appetite for loss. If a firm has not performed this exercise and believes it may be a disproportionate step to undertake such an exercise a practical step could be to qualitatively assess the bands in terms of behaviours (i.e. at what level historically have the Board, CEO, CFO asked for detailed information – this level could serve as a proxy for the lower bound of "high", and the level at which a capital injection might be necessary could serve as the lower bound for "very high", "extreme" or another superlative as appropriate.

- Firms should consider whether it is more efficient to have the risk department hold the pen for the RCSA or to syndicate the task to the business units and submit the RSCA to the risk department for review and challenge.

- Firms should take advantage of this exercise and use the RSCA to track their risks, controls and the actions that are required to bring residual risk within risk appetite and share the higher residual risks and the associated actions with the governing body

5.2.1.1. Table 2 – Examples of good and poor RCSA practices

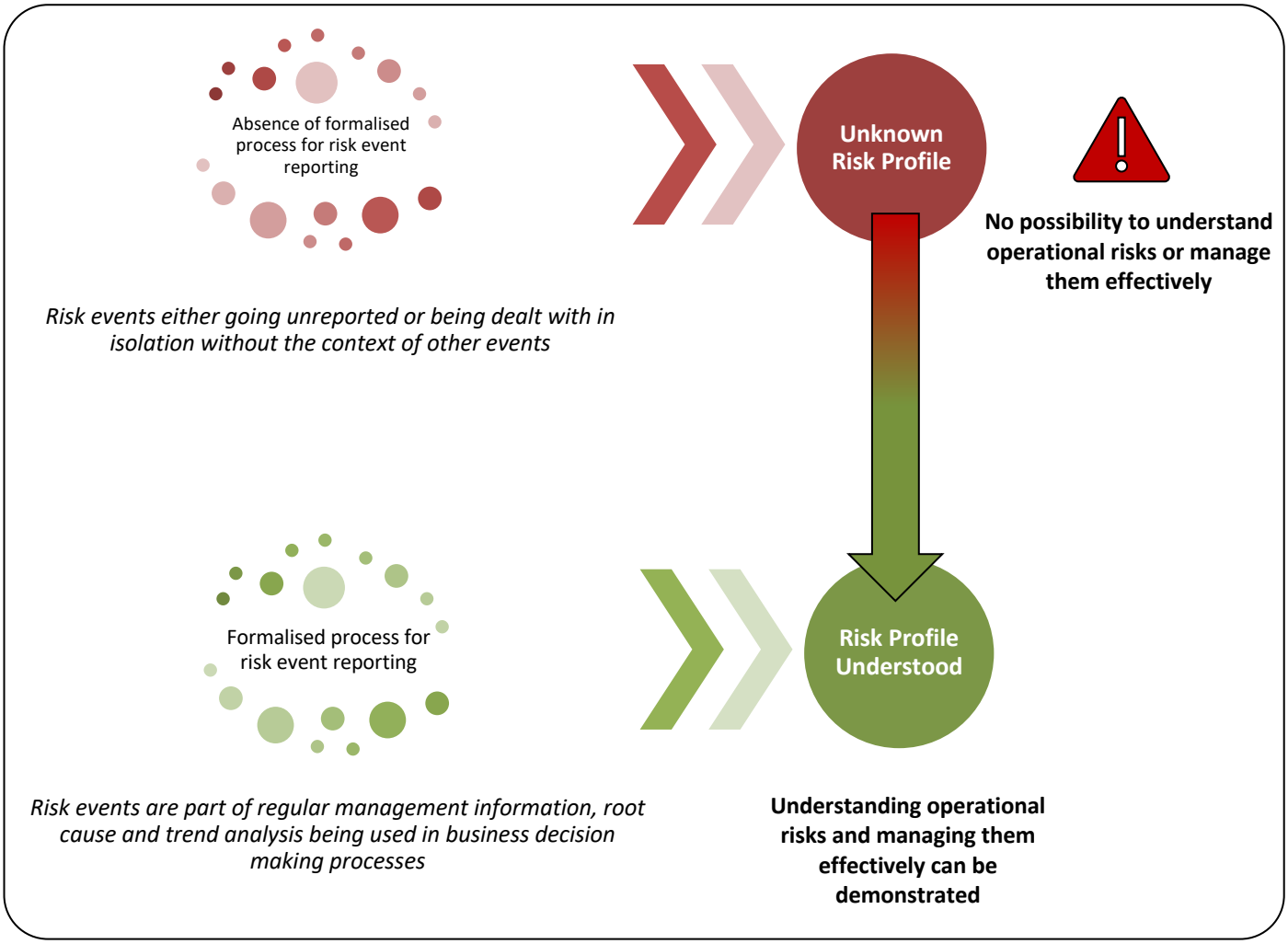
Examples of good practice	Examples of poor practice
Senior management are seen to actively sponsor the RCSA process, and middle management ensure the RSCA process is prioritised within the day-to-day activities.	The RSCA is seen as something the risk or compliance department are responsible for, other areas are not incentivised to engage in the task, nor is the task prioritised by the middle management.
RCSA are used to track the risk profile at business unit level periodically, actions are followed up and high-risk items and risk acceptances are managed in one place.	The RSCA is a one-off and standalone exercise, the data is not used other than once a year when the Board or regulator ask to see a risk assessment.
With respect to the REP 018 operational and security risks are additionally assessed in terms of a firm's ability to responds and recover from an event (i.e. consider business continuity) and the risks associated with business disruption are considered in the round, in context of other risks in the risk register.	The REP 018 is a one-off exercise that does not consider incident response and recovery, and the scenarios considered for business disruption risks are limited to loss of access to employees and premises.
There is consistency between the risk register and RSCA, the risk terminology is the same and the activities that lead to the risks are clearly articulating alongside the controls that are designed reduce and/or control the risks.	It is difficult to see traceability between the RSCA and risks in the risk register. It is not clear as to how the activity leads to the risk, nor is it clear as to how the control related to the risk.
There is consistency between risk appetite, residual risks, actions and target timeframes (e.g. if a residual risk is outside risk appetite there is an action that is owned by a senior manager with a target timeframe to reduce the risk, or remove the risk acceptance that is commensurate with the Board's need to bring the risk profile back within risk appetite).	There are either no actions arising from the RCSA, or the actions that are recorded do not obviously serve to reduce the risks. The actions are delegated to such a low level in the firm that the probability of delivery is low, and there is no senior management accountability.
Controls are marked as preventative or detective, it is obvious that both types of control exist for each activity that could lead to risk, and where both types of control do not exist there is either an action or a justification. Controls are marked as effective or ineffective, and there is evidence to support a controls status. There is a schedule in place for controls testing for those activities that have been assessed as higher risk.	Controls are not categorised or tested, or there is no evidence of controls testing.
There is evidence of risk event and loss event data being used to assess the residual risks and when there is a risk event or loss event the information in the RSCA that is relevant to the event is demonstrably reassessed; or the RSCA is updated to reflect any new controls implemented as a result of the event.	The RCSA and risk event, loss event reporting process do not seem to be linked in any way and the processes run independently of each other in silos.

5.2.2. Risk event and loss event reporting

Risk events[10] (sometimes referred to as incident reporting or loss event reporting) are fundamental to any ERMF and most, if not all, firms will have processes in place to escalate losses. However, some firms may take the view that because they are small, co-located with senior management, or have a good track record for operational losses that having a more formal process for risk event reporting is unnecessary. An ERMF cannot deliver the benefits alluded to in section 3.3 unless risk event reporting is formalised, and trends analysed.

Figure 2 – Purpose of risk event reporting

The primary purpose of risk event reporting is for a firm to understand its operational risk profile. The risk event data is also likely to be part of any request for information from FCA as part of any governance, controls and risk management framework review they may undertake at a firm.



[10] A risk event is any event that was an unexpected outcome. An internal risk event is an unexpected outcome that has its origin or impact inside the firm, and external risk event is one that has both its origin and impact outside the firm. Internal risk events should be recorded in cases where there has been, or there may be a financial loss or unexpected cost in the future

- Firms should have a formalised process for risk event reporting which is supported by management information for the governing body.
- Firms should consider how best to consolidate risk event reporting with other types of reporting (e.g. compliance breaches and/or system outages).
- Firm should keep records of actual financial losses or unexpected costs that materialised as a result of the risk event(s), and where there were no actual financial losses or unexpected costs estimate what the potential might have been had the event been under slightly different circumstances or progressed in some way.
- Where there was an actual financial loss, which was subsequently recovered (e.g. funds sent to the incorrect beneficiary, subsequently recovered in full), the amount before recovery should be used to estimate risk impact.
- When setting the thresholds for what might be considered a "Low", "Medium", "High", or "Higher" impact risk event a firm should set these thresholds consistently with those that appear in the RSCA templates (or other risk assessment method that the firm chooses to use).

5.2.2.1. Table 2 – Examples of good and poor risk event reporting practices

Examples of good practice	Examples of poor practice
There is a formal risk event reporting process in place. Management information is submitted to the governing body in a consumable form, risk events are categorised in a consistent (if not the same) way as the risks are described in the risk register.	There is no formality, management information sporadic and generally only available when there has been a large loss, or the concern that there will be an unbudgeted cost as a result of the event.
Detailed root cause analysis is performed for at least the high risk (or potentially high risk) events, this information is then replayed into the RSCA process, the actions arising recorded in the RCSA and the residual risk reassessed as a result of the event.	There is little effort to establish the root cause and solutions are often a "knee-jerk" reaction with no reference back to the RCSA or other risk management tools.
The task of reporting risk events is syndicated throughout the organisation and adopted by all areas in the firm. More sensitive matters (such as those that relate to conduct or suspicious activity) are recorded as risk events the details recorded in the most appropriate place (if not the risk event reporting data storage solution) itself).	Reporting risk events is seen as the risk and/or compliance team responsibility, there is no buy-in unless "someone else" does it, and other areas such as HR, and Compliance themselves make no attempt to consolidate the events they deal with on a day-to-day basis with the other events that the risk event reporting process is designed to capture and analyse.
The management information in place for risk event reporting is demonstrably used for making investment decisions, setting priorities and is sponsored by, not only the Board, but the CEO, CFO and other members of the senior management team.	The management information is presented to the governing body in isolation, often towards the back of the papers and no consideration is given to the risk event data when making investment decisions as to people, processes and/or technology.

5.2.3. Key risk indicators and performance indicators

Key risk indicators ("KRI") and key performance indicators ("KPI") are fundamental to running a business in as much as they allow the Board and senior management teams to monitor the rewards as a result of taking the risks. Revenue, profit and loss arising from risk rather than the other way around.

Generally speaking, firms will have well developed processes for monitoring performance against a budget and various other documented processes and management information to support revenue recognition. In part this is because their accounts need to be audited, but more importantly it is because a business needs to remain profitable for it to grow (growth being a key objective for any CEO or CFO).

It is also the case that where a firm takes market, credit or liquidity risks the processes supporting this type of management information is also relatively mature, in part because these types of risk are easily related to financial performance metrics and because there are well defined regulatory reporting processes that need to be followed (e.g. periodic regulatory capital returns where these are the risk drivers for changes to the numbers).

In a mature ERMF, these types of KRI and KPI are discussed alongside operational risk metrics to provide an entreprise view of the risk profile and to provide some certainty as to the quality of those other metrics. The question is asked, when assessing operational risks – how well controlled are the processes that support our financial performance and risk metrics? The management information that relates to operational risk metrics answers this question.

A KRI should also be used to assess and quantify the operational risk profile (by category of risk) in order for the senior management team to ascertain where the firm is against the Board's stated risk appetite. Risk event data can also be used to make this assessment.

- Firms should as a minimum have a KRI, to quantitatively assess the risk profile against the Board's stated risk appetite for each category of risk that has been identified.
- Firm should consider how many they need for each type of risk that they are exposed to and include the Board in the decision-making process.
- Firms should set thresholds for each KRI that are designed to capture high utilisation (AMBER), and at what level they should set them to avoid being surprised by being outside of risk appetite (RED).
- Firms should consider how best to represent KRI data and which KRI goes to which forums to avoid overloading the governing body with duplicative data and/or a level of detail that cannot be consumed.
- In the context of conduct risk management, firms should consider the design of non-financial KPI for client facing employees as part of the ERMF.
- Firms should look to use visual representations as much as possible and attempt to draw conclusions from trends, rather than solely focussing on a period end close of business date.

- With respect to financial risk metrics (those for market, credit, liquidity risks)
    - firms should understand how they take market risk, and what if any business practices they have that create contingent market risks and put metrics in place to monitor these levels of market risk.
    - firms should measure credit exposures at legal entity, and total credit exposure to a group be able to create trend analysis over time,
    - firms should take a risk-based approach to granting credit and assess different types of clients in different ways to assess their credit worthiness,
    - firms should be able to identify and measure concentrations of credit risk,
    - firms should consider whether credit exposure limits are appropriate for the type of business activity they undertake and should be able to monitor residual credit risk exposures[11],
    - firms should consider how to aggregate credit exposures in such a way that they are able to assess the total credit risk exposure taken,
    - firms should assess their liquidity exposures at least daily, and set KRI that are consistent with their liquidity resources that are *immediately available* (e.g. cash at bank, revolving credit facilities etc.), and
    - firms should consider setting liquidity limits, that are consistent with the types of exposures that arise from its business activities (e.g. variation margin, chargebacks etc.) and *monitor* exposure on a near real-time basis, and report any instances where exposure was outside limits
    - firms should consider how they would calculate any liquidity buffer requirements that are either part of their regulatory requirements, or as a result of the Board's desire to hold a liquidity buffer

[11] Residual risk in this context being the risk that credit risk mitigation techniques are not as effective as expected

5.2.3.1. Table 3 – Examples of good and poor KRI and KPI practices

Examples of good practice	Examples of poor practice
KRI reports are clearly linked to risk appetite statements and are set at thresholds that are commensurate with the risk appetite statement (e.g. zero risk appetite = > 0 events is outside appetite).	KRI reports do not have obvious links to risk appetite and/or there is no context or justification for the thresholds that have been set.
KRI reports have high utilisation thresholds, reference risk events, the direct or indirect financial impact and there is an explanation as to the path back to a lower utilisation, or a formal risk acceptance in place	There are no high utilisation thresholds other early warning signs, nor is there any evidence of a discussion or plan to reduce the risk profile or accept the risks.
KRI reports are timely (i.e. they reflect the current risk profile) and the frequency of reporting of the KRI is commensurate with the rate of change of the risk being measured (i.e. financial risk metrics are likely to change daily and therefore should be measured and reported daily, the should be analysed throughout the reporting period)	KRI information is significantly out of date by the time it is published to the governing body (e.g. credit utilisation from 6 weeks ago with no trend analysis or more recent insight)
KPI and KRI reports are linked appropriately, appearing on the same page in context where it is appropriate to do so (e.g. credit exposure to a customer alongside revenue associated with that customer, or volume of payments alongside number and loss impact of payment errors). It some cases it may also be appropriate to report number of risk events, conduct and/or compliance breaches alongside a revenue generating areas revenue or profit and loss.	KRI reports and KPI reports are separately completely and it is difficult to see how the risks and rewards are related. It may even be the case that performance indicators are not shared with or discussed in any forum that includes control functions.
There are non-financial KPI reports and incentives to hit non-financial targets (such as training completion, or quality of suitability assessments) in addition to financial KPI reports that focus purely on growth and revenue targets	KPI reports focus solely on financial targets

5.2.4. Scenario analysis and stress testing

Scenario analysis and stress testing is a vital component of an ERMF as it is pro-active, forward looking and gives firms the opportunity to either avoid risk events entirely or plan for them careful in an effort to reduce impact. The most common form of scenario analysis uses external risk events (events that have had their impact and origin at another firm, e.g. regulatory enforcement, a data breach, a publicly known credit loss etc.).

The external risk event approach is useful because it is factual rather than hypothetical and there is usually a wealth of information available. This is an analysis that attempts to answer the question "could it happen here?". The firm can then consider what control gaps it might have and prioritise its investments accordingly to avoid such an issue or reduce its impact.

Another approach is hypothetical scenario analysis. This is useful because it can be tailored specifically to a firm and using internal data a firm can choose the risks it would like to assess this way (usually its higher risk activities) and analyse how something could go wrong, how bad it could be and then consider what it could do to avoid these hypothetical events from taking place and/or how to reduce the impact should they occur.

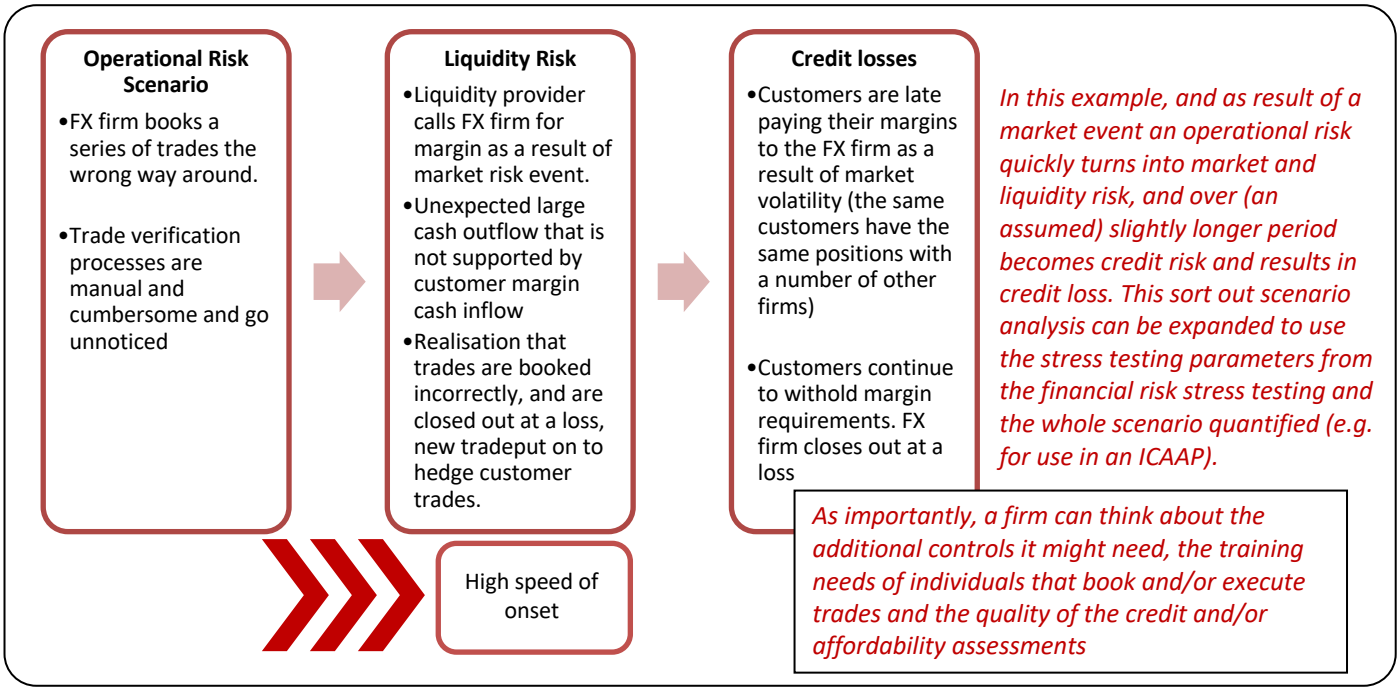
Scenario analysis is generally the approach taken for operational risks, although there are some instances where stress testing would more appropriate to prepare for or avoid an operational risk, risk event. A good use case for stress testing could be to avoid a business disruption event by load testing a platform in anticipation of increased volumes of transactions during market volatility, or too estimate the operational capacity of a client on-boarding function in anticipation of higher new customer demand.

Notwithstanding its application to other risk types, stress testing is generally used in relation to financial risks, and financial risk management and (e.g. move the FX market X% and see what impact this has on a firm's credit exposures and liquidity position).

Scenario analysis can also take a more practical form where facilitated sessions that imagine an event has taken place and ask delegates to role play out what they would do, in some cases asking delegates to physically contact other individuals, or physically bring the information back to the room where the facilitated session is taking place. This type of scenario analysis is most often used in incident response and recovery training, again for hypothetical business disruption scenarios but can also be applied to other hypothetical events such as a material credit or liquidity event.

- Firms should undertake scenario analysis for all key risks, or activities that are considered higher risk.
- Firms should consider which external risk events are most relevant to them and how to best assess the likelihood and impact of the same, or similar, event taking place internally.
- Firms should combine scenario analysis with stress testing and assess the impact in the context of its capital requirements
- Firms should consider the benefits of scenario analysis that take the form of role play and run facilitated sessions the output of which should also be documented
- Firms should explore the interconnected nature of risk (i.e. one risk turns into another) as part of the scenario analysis in order to evidence a holistic approach and demonstrate the understanding that it is rarely the case that risk does not take on other shapes as can be seen in figure 2.

Figure 2 – Illustration of how scenario analysis can elucidate the interconnected nature of risk



5.2.4.1. Table 4 – Examples of good and poor scenario and stress testing practices

Examples of good practice	Examples of poor practice
External risk events are sought out, analysed and the question "could it happen here?" is answered. Analysis of events is not restricted to the same *specific* sector (i.e. it happened at bank therefore it is not relevant), instead events are analysed based on the risk that manifested rather than the firm it manifested in.	External events are not highlighted or analysed in any detail. External events are highlighted and analysed to an extent, but only in cases where the event has taken place at a direct competitor.
Scenario analysis is sponsored and led by a senior individual at the firm its output is documented, for higher risk activities presented to the governing body formally and the actions arising are owned by a senior individual and progress tracked There is a proportionate response to the results of the scenario analysis, and should higher risk gaps be exposed, and high priority actions assigned the actions are resourced appropriately and the risks accepted by the appropriate senior manager whilst the actions are delivered.	Scenario analysis either does not take place at all, or is implied through anecdotal internal storytelling, hyperbole or a refusal to entertain the possibility that such things could happen. It is sometimes the case that senior management or Board members create an environment that if a hypothetical scenario is mentioned it is taken to mean that there are no controls in place and results in a disproportionate response and excessive resource expenditure. This can result in reluctance to consider scenario analysis as a good risk management tool.
Stress testing parameters are well thought through, have some basis in either historical time series (e.g. market moves) or a realistic expectation that a stress event is plausible. The parameters are regularly reviewed, and the results acted upon by senior management.	There is no basis for the stress testing parameters, or that basis was established too long ago for it to be considered (by an external party) relevant; or the stress testing parameter are so severe to make them either implausible, or if they are accepted the results ignored by senior management.

5.2.5. A policy framework

With respect to risk management (in the context of this guidance) AFEP would expect its members to have at least the following documented policies or policy statements within an overarching manual, or ERMF document.

- Risk event reporting policy, and procedures for reporting a major incident[12]
- An Operational Resilience Framework[13] including an IT Security Policy, and Business Continuity Policy supported by Business Impact Assessments
- Policy statements as to how market risks can arise and (depending on individual firm permissions) how these market risks must be minimised. This policy statement should consider business practices that might lead to market risks.
- A Credit Risk Management Policy
- A Liquidity Risk Management Policy (or similar document that outlines a contingency funding plan)

5.3. The Use Test

The use test in regulatory parlance is the process by which a firm demonstrates effective risk-based capital management, strategic risk management and decision-making. In business terms, the ability to demonstrate that the information from the ERMF is being used in the day-to-day running of the firm, and the business planning process.

When the CEO, CFO, other senior managers and Board members can explain the ERMF and can evidence that they are using the framework and its outputs to support their decision-making processes it is not a "box-ticking" exercise. From a purely commercial perspective once a firm has invested in the design and implementation of an ERMF it makes sense to use the investment.

Adopting these guidelines and following the example of good practice will put member firms in good standing for passing the use-test and, more importantly, will position a firm well to take advantage of the key benefits alluded to in section 3.3 repeated in this section for convenience.

A. Protect revenue and maintain profitability.

B. Identify and prioritise activities that bring the highest risks and direct human and technology resources towards these risks by using internal data.

C. Drive down the likelihood and impact of operational losses, unexpected costs and in so doing, for the same revenue, increase profitability in the medium to long term.

[12] In July 2017 the EBA published its Final Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) the guidelines were transposed into UK law in December of that year and FCA noted their intention to adopt these guidelines three months earlier in September 2017 through their policy statement SUP 15.14

[13] AFEP intends to create a good practice guidance document for Operational Resilience during the second half of 2020

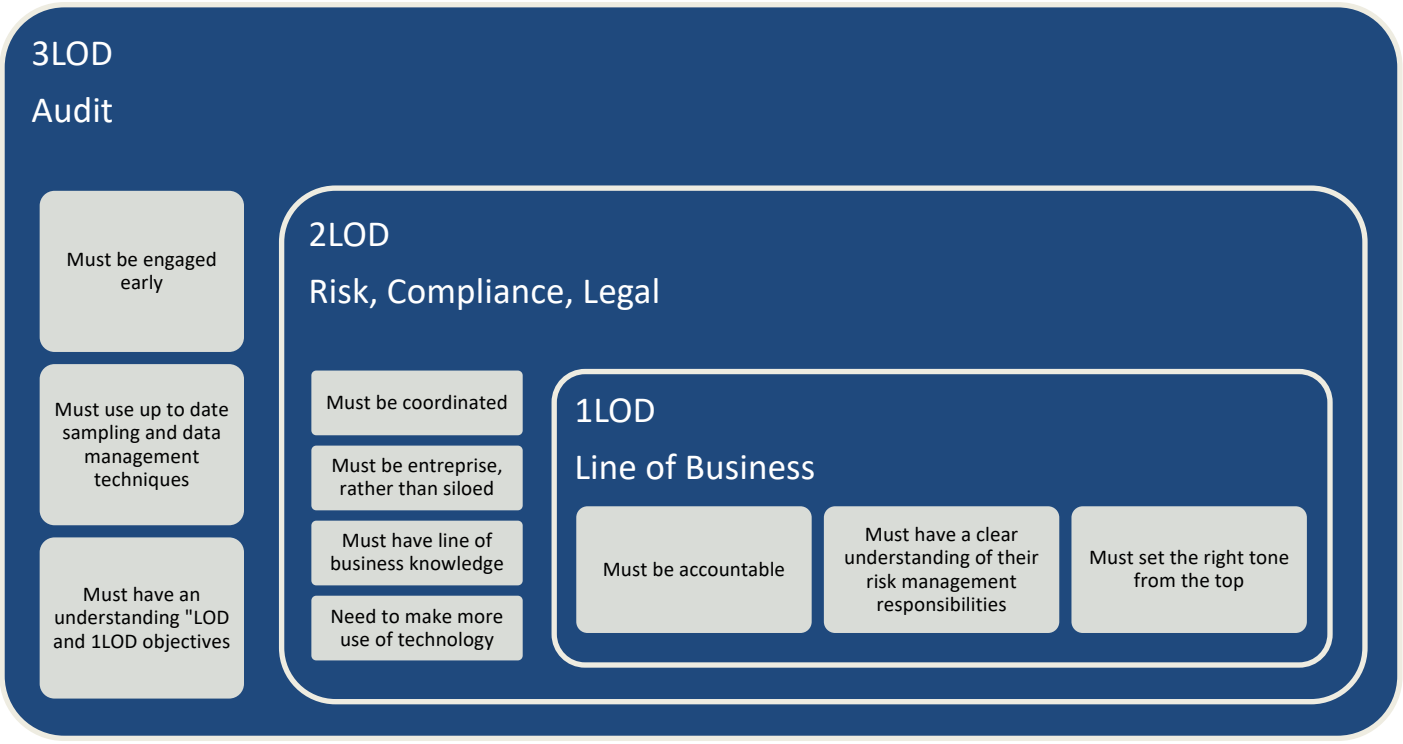
6. The three lines of defense model

AFEP members will either have or will be building a "three lines of defense model" (1LOD, 2LOD, 3LOD). Traditionally, Front-office, Operations and IT is 1LOD, Risk, Compliance, Legal and certain areas in Finance are 2LOD and Audit functions are 3LOD.

Risk management activities form part of a control framework. A part of this control framework is the requirement to assess the risks to achieving the objectives and implement and maintain such processes including controls that senior management deem necessary to manage, control and monitor risks, and to carry out some assurance that the processes and controls that are in place are effective. 1LOD and 2LOD activities should be developed in line with this risk management good practice guidance.

- 1LOD includes the actions of the individual, front-office and other lines of business teams. Front-office and, to an extent, Operations and IT teams are the "risk takers". It is important for senior managers to understand how 1LOD actions affect the control environment, and what controls are operated by the 1LOD themselves.
- 2LOD is higher level assurance to assess the effectiveness of business processes, operational controls and management controls in ensuring compliance with processes, controls and external laws and regulations. These activities are designed and directed by the business but performed independently from the direct management of the actions.
- 3LOD relates to and additional and more independent review and challenge of the 1LOD and 2LOD functions and is provided by internal and external audit.

Figure 2 – Illustration to outline good three lines of defense practices



7. Risk management good practice checklist

AFEP are not advocating simply producing a checklist and applying a tick box ideology to risk management. However, AFEP does believe there is some value in producing a summary checklist for firms to reference against. See below.

7.1. Table 5 – Risk Management Summary Checklist

Key Activity	Ownership
Document the approach to the governance structure and set up at least one formal committee to oversee risk management activities and the outputs from 1LOD, 2LOD and 3LOD.	Board supported by 2LOD.
Create the risk register and assign senior management owners. Use industry standards, we have recommended using the loss event categories documented in the CRR as a start.	2LOD create risk register, C-suite take ownership.
Appoint a senior manager in 1LOD *and* 2LOD who will be responsible for the ERMF itself, document the shared responsibility[14]	The Board
Document the approach taken to the components of the ERMF	2LOD to create the document, C-suite to review and Board to approve.
Create and populate the RCSA and Controls Library. Note that this exercise is wider than the REP018, the REP018 being primarily a security risk assessment.	2LOD to lead in the first instance with the intention to hand ownership to 1LOD.
Create and approve a risk event reporting policy, collect and analyse the data. Report this information to the governance forum. Consider whether a technology solution is necessary[15]	2LOD to oversee this process. Risk events should be logged by the team in which they originated.
Create a risk appetite statement document and assign metrics to measure the risk profile against the risk appetite	2LOD to facilitate discussions with 1LOD and Board. The Board are responsible for implementing risk appetite.
Ensure there is management information coming from all areas of the firm, do not expect 2LOD to produce all the risk management information.	C-suite need to sponsor this ideology.
Combine key risk indicators with key performance indicators. Present the revenue in the context of the risks being taken to achieve the revenue (e.g. number of options sold next to number of suitability assessments that met the expected standard)	C-suite need to sponsor this ideology.

[14] Where a member firm has an entity that classified as "enhanced" under SMCR certain prescribed responsibilities (e.g. those of the SMF 4 and SMF 24 if they are to be shared, there must be a clear rationale and no overlap of responsibilities).

[15] Based on some member feedback once there are more than 100 risk events logged managing the data in spreadsheets can become onerous and technology solution becomes more cost effective, especially where the Board require infographic style outputs.

8. Examples of risk management failures and the consequences of getting it wrong

Understandably unless there has been a public censure or press headlines, factual, rather than anecdotal or speculative, information as to risk management failures and consequences of getting wrong is difficult to curate. There have been very few headlines relating to firms in the specific sector (FX Payments Services) to which this guidance relates. However, as proxy "Skilled Persons Reviews" are good example of at least the perception of a risk management failures.

Section 166 of FSMA (s166) gives the FCA the power to get an independent view of aspects of a firm's activities that cause FCA concern or if FCA need further analysis. Either the firm or, under the Financial Services Act 2012, the FCA can appoint the skilled person firm(s) to do this. In each case, FCA set the scope of the review and the firms pay the costs.

AFEP is inclined to assert that if a firm is subjected to an s166 there has been a risk management failure of some sort, whether or not there is enforcement action. This is not to say that the risk management and/or compliance team has failed in every, or indeed *any* specific case. It is, however, sometimes the case that FCA intervene in an attempt to avoid a more public failure of a firm's risk management framework.

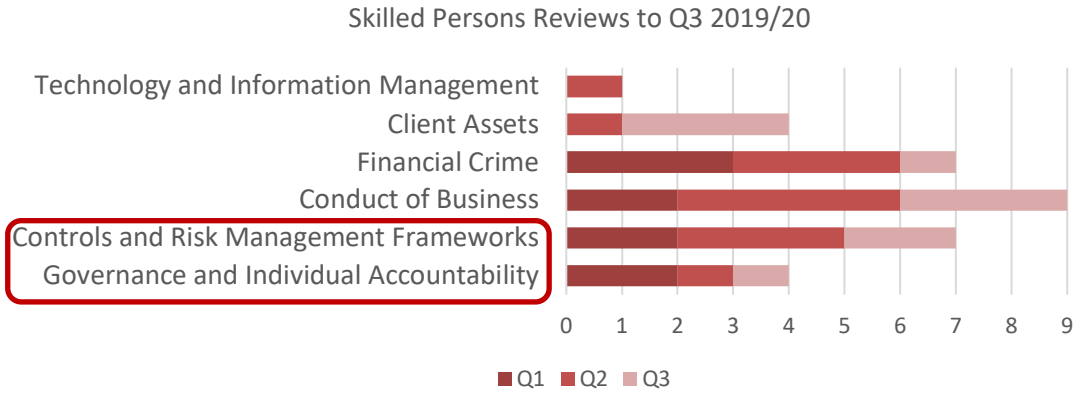
Of the 34 s166 issued in 2018/19, 7 were as a result of FCA concerns as to a firms "controls and risk management framework", the FCA provided some further commentary in their Annual Report, going to say that these reviews also included "adequacy of systems and controls, including the effectiveness of control functions". 1 was issued for "governance and individual accountability"

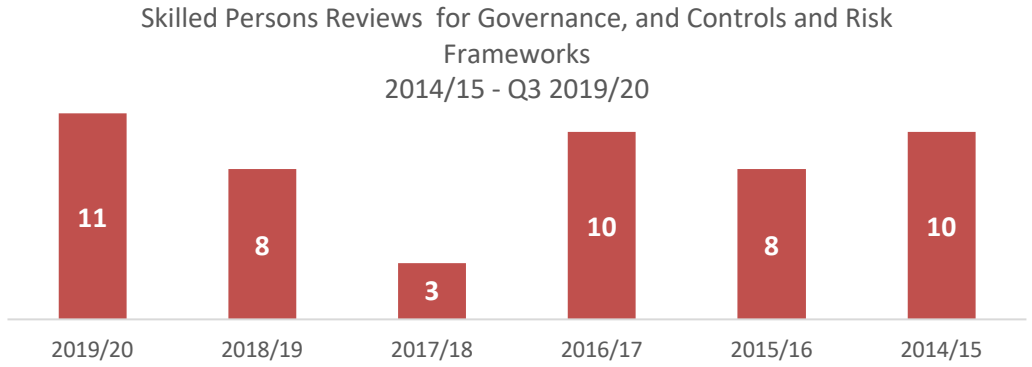
During 2019/20, based on FCA reported information to date, FCA have issued a total of 32. 4 of which were for "governance and individual accountability" and 7 for "controls and risk management frameworks".

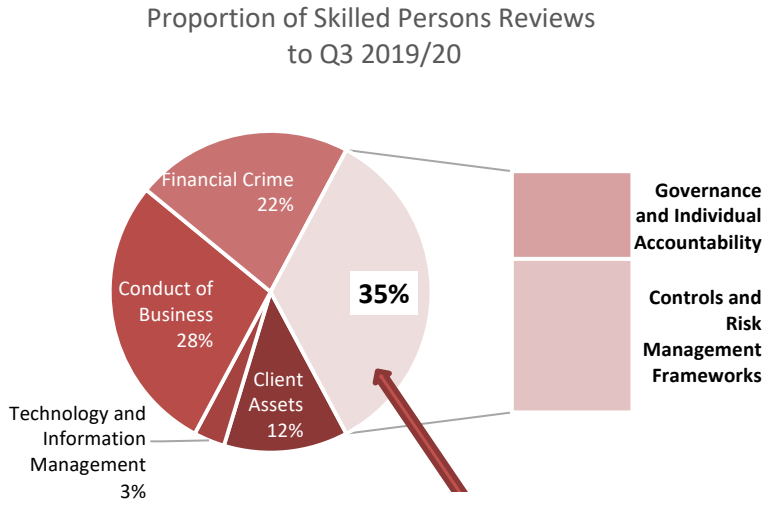
Put another way 35% of the skilled persons reviews during 2019/20 are in some way related to the subject matter in this good practice guidance.

Skilled persons reviews take place at firms' expense, they are costly, tie up an enormous amount of management time and with respect to those issues for Controls and Risk Management Frameworks can be easily avoided. In some cases, skilled persons reviews can lead to regulatory enforcement against the firm or individuals.

8.1. Figure 3 – Skilled Persons Reviews







FCA separated Governance and Individual Accountability from Controls and Risk Management Frameworks in 2017/18. They have been combined in the graphic (left) for comparative purposes.

The single largest proportion of skilled persons reviews to Q3 2019/20 has been for matters relating to governance, controls and risk management frameworks.