EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Digitalisation: key assessment criteria and collection of sound practices

1 Introduction

Digitalisation is a structural trend affecting European banks. They are adapting to changing customer preferences, new technologies, a different competitive landscape – with new entrants in the financial markets – and changes in the value chain. Digitalisation is impacting banks' front office and back office operations – as they are offering new digital products and services while automating internal processes. It is also affecting their risk profiles, including strategic and operational risks but also financial risks depending on the digital activities. ECB Banking Supervision is closely following developments such as digitalisation that are likely to affect euro area institutions and updating its methodological toolbox to assess related risks.

This is why ECB Banking Supervision included digitalisation in its priorities for 2022-24 and again for 2023-25 in order to address digitalisation challenges, related risks and management body's steering and risk management capabilities. While supervised institutions should keep a strong focus on addressing structural challenges and risks stemming from the digitalisation of their banking services with a view to ensuring the resilience and sustainability of their business models, ECB Banking Supervision is assessing the related risks, how they are identified, monitored and mitigated.

Building on the market intelligence discussions with banks and key market players, and the survey on digitalisation involving all significant institutions under European banking supervision conducted in 2022, a broad set of supervisory activities was completed in 2023. These included targeted reviews on the steering of digitalisation covering 21 banks, 10 on-site inspections on digitalisation (5 in 2022 and 5 in 2023), and the assessment of digitalisation data collected through the short-term exercise (STE) and for the Supervisory Review and Evaluation Process (SREP).

These activities have further allowed ECB banking supervision to assess banks' digitalisation activities and related risks. The starting point for such an assessment is the general framework outlined in the Capital Requirements Directive (CRD), as implemented in national law, together with the relevant European Banking Authority (EBA) guidelines – in particular, on the SREP, outsourcing and internal governance. Along with these the ECB considered the publications of international and European standard-setting bodies on digitalisation and technology-related risks. Some consistently applied "sound practices" of SSM banks – approaches the ECB has observed to generally meet the assessment criteria – have also emerged. These are being published today at an early stage, in order to inform the supervisory dialogue on those aspects with the banks making a strategic decision to develop their digital footprint. As part of this supervisory dialogue, the ECB will discuss with institutions

the ECB's assessment criteria in terms of any possible divergences in institutions' practices.

The assessment criteria and sound practices set out below are grouped together according to three themes: business model impact, governance and risk management. These criteria and practices may be further fine-tuned based on upcoming supervisory activities, including future targeted reviews, on-site inspections and deep dives.

Sound steering of digitalisation: key assessment criteria for institutions' business models, governance and risk management

Institutions assessed as adequately steering digitalisation had taken the following steps:

1. understanding the impact of digital trends on the business environment in which institutions operate in the short, medium and long term, in order to be able to make informed commercial and strategic decisions;

2. based on an informed perspective, deciding on the need to formulate a clear and well-articulated digital strategy, and defining strategic objectives that are to be achieved by means of digitalisation and innovation;

3. having in place adequate financial and non-financial execution capabilities for a proper implementation of the digital strategy as defined;

4. developing a comprehensive framework of financial and non-financial key performance indicators (KPIs) for monitoring the implementation and execution of the digital strategy and for reassessing it in the event that targets are missed;

5. having a clear allocation of responsibilities related to digital topics in the management body, whether individual allocation to those with a management function/executives, and/or senior managers reporting to the executive management, or a dedicated centralised steering/coordination body, enabling adequate coordination of digital initiatives at group level;

6. setting up adequate processes covering all subsidiaries and business lines: defining the business areas ultimately responsible for reporting on digitalisation initiatives and setting up top-down steering and monitoring processes and proper bottom-up reporting processes,

7. having a management body with a supervisory function/non-executive role that constructively challenges the management body in its management function/executive level role and provides effective oversight of the digitalisation strategy and related risks;

8. assigning internal control functions a strong role in the digitalisation process, new product approval process (NPAP) and ongoing business operations, while ensuring their independence;

9. embedding digitalisation in the risk culture (e.g. tone from the top, incentives, risk accountability and a culture of challenge), both top-down and bottom-up, including the communication on strategy and risks, thereby creating awareness and fostering knowledge;

10. ensuring insight and monitoring of critical dependencies, interdependencies and third-party relationships, and not only of outsourcing, on an ongoing basis;

11. having in place a data governance process to support data-driven digitalisation activities;

12. carrying out a detailed impact review on traditional and non-traditional dimensions of risk during the process of digital strategy-setting and the NPAP as well as during the execution of the digital strategy;

13. assessing and updating all dimensions of the risk map, reviewing the suitability of existing risk models in view of digitalisation and adapting them as necessary;

14. reviewing the risk appetite framework (RAF), the risk management framework (RMF) and the key risk indicators (KRIs) defined ex ante and adapting them if needed in view of digitalisation initiatives.

2 Assessment criteria relating to business models and strategy

Articles 73 and 74(1) of the CRD, as further specified by the EBA Guidelines on internal governance, require institutions to implement internal governance arrangements, processes and mechanisms to ensure effective and prudent management of the institution. In this respect, it is important for institutions to identify, assess and monitor the current and forward-looking impact of digital trends on their business environment and to ensure that any digital strategy they pursue is properly coordinated, steered and monitored.

2.1 Business environment

Assessment criterion 1: Does the institution understand the impact of digital trends on the business environment in which it operates, in the short, medium and long term, enabling it to make informed commercial and strategic decisions?

Assessment criterion 1.1

Does the institution identify, assess and document, in a comprehensive and systematic manner, the digital-related external factors impacting its business environment? These factors include the competitive landscape, policy and regulation, innovative technologies and customer preferences, also based on socio-demographic factors.

Moreover, does the institution perform a digital readiness assessment to understand its digital positioning? The digital readiness assessment entails gaining an understanding of internal factors, such as the availability of financial

resources, human capital and skills, the complexity of legacy systems and the use of innovative technologies.

Assessment criterion 1.2

Does the institution understand how digitalisation affects its business environment in the short, medium and long term and does this awareness inform its business strategy process? The way that institutions strategically respond to changes in their business environment stemming from digitalisation may impact their business model over time.

Institutions therefore need to explicitly consider digital trends even if they may decide against pursuing a digital strategy. This would be reflected in institutions' business strategy processes and demonstrated by documented management body meetings and discussions.

Box 1

Examples of observed sound practices: comprehensive business environmental analysis

The ECB identified a comprehensive strengths, opportunities, weaknesses and threats (SWOT) analysis as a sound practice. For instance, some institutions organised the SWOT analysis across the following pillars to inform their digital strategies:

- clients' behaviours, expectations (monitored for instance through specialised regular market benchmarks or continuous client feedback) and the demographic implications of the institution's client base, which help tailor its offer to specific audiences;
- competition insights (trends or market approaches in terms of offer and distribution) to allow a competitive analysis also covering non-banks (fintech, bigtech, e-commerce, retailers and utilities) and the evaluation of potential collaborations and partnerships;
- regulatory requirements and their implications, to ensure due compliance, to force reprioritisation dynamics into the original roadmap and scan for opportunities for innovation;
- operating model and support capabilities, to ensure that the current organisational set-up and those internal processes impacting the execution of digital strategy are effectively supporting digital development;
- cybersecurity and data protection considerations, to ensure that the digital strategy safeguards customer data and a secure online environment, while adapting to evolving threat patterns and technological advancements;
- technological developments and potential risks (the IT team, together with digital and business teams, monitors new technologies and performs sandbox testing of technologies considered relevant in terms of their potential applications in the short and medium term);
- technological infrastructure and innovation capabilities, to ensure alignment with the business strategy objectives and digital implications in terms of innovation, resilience and long-term agility;
- data and artificial intelligence (AI) capabilities, to spot opportunities for automating internal processes and improving customer services;

- the maturity of the current digital capabilities, to spot gaps in digitalisation coverage and opportunities for major improvements in customer journeys;
- digital talent acquisition and development, to enhance the institution's ability to implement its digital strategy effectively and maintain a sustainable pace of transformation.

The ECB observed that a few institutions have a group strategy, technology and innovation department in charge of developing a trend book covering technologies, products, business models, client behaviours and competitors' strategies. The trend book is reported to the Board of Directors and serves multiple purposes:

- ensuring that the institution makes appropriate and timely investments in specific trends;
- guiding subsidiaries in different geographical areas in setting priorities and defining strategies;
- providing continuous evidence of the validity of the strategic assumptions and serving as an input for their regular update – there is also a methodology for clearly indicating those trends where greater effort is needed to safeguard profitability and the competitive position.

An additional sound practice observed by the ECB is an external market analysis accompanied by customer satisfaction measures, with dedicated input from the customer complaints team.

By analysing past patterns of complaints, this approach helped predict which changes could result in spikes in complaints. The input was considered before the development of new digital initiatives. For critical initiatives, a dedicated quality management expert from the complaints function assisted the development team. The quality management function was also often involved afterwards, reacting to unusual complaint clusters related to digital migration. For example, when introducing new automated banking terminals in branches a task force was created to address and avoid the potential increase in complaints, and improve customer experience.

This resulted in: a new design for the banking terminals, a plan for reviewing the implementation after one month, internal communication and the introduction of more terminals in high-stress branches.

2.2 Digital strategy formulation and definition

Assessment criterion 2: Does the institution – based on an informed perspective – take decisions on the need to formulate a clear and well-articulated digital strategy, defining strategic objectives that are to be achieved by means of digitalisation and innovation?

The ECB has a neutral stance on the format of the digital strategy: it can be embedded in the business strategy or the IT strategy, or it can be a standalone document.

Assessment criterion 2.1

Does the institution make a clear decision on whether to formulate a digital strategy? If so, does the digital strategy set out clear strategic objectives to be achieved through the application of digital technology solutions? Clarity on

digital strategic initiatives implies understanding how the use of technology can support business initiatives, ultimately boosting the performance of the institution.

A well-articulated digital strategy identifies: the key digital initiatives and their alignment with the long-term business strategy; the key technologies underlying key digital initiatives; quantitative profitability targets for key digital initiatives or, if this is not possible, an understanding of the value they generate by enabling other strategic initiatives; and a granular definition of the strategy at all the relevant levels of the institution (such as geographical areas, business lines and sectors).

Box 2

Examples of observed sound practices: a clear and well-articulated digital strategy

The ECB observed some institutions that had a clear digital strategy embedded in their business plan. Digitalisation plays a key role in the business plan as enabler of strategic priorities.

For instance, one good practice was defining clear strategic priorities on “reinventing the customer experience” (personal banking in the digital age, with a focus on client groups that value expertise and relationships) and “building a future-proof bank” (rationalisation, digitalisation and automation further enhancing customer service, compliancy and efficiency). This was underpinned by:

- a new targeted operating model outlining how the approach would work internally, covering aspects of client experience such as: i) clients being serviced through a new three-layer model – first digital, then remote, then personal support; ii) reducing the number of products by a given percentage; iii) standardising a digitalisation cluster for customers, product and internal processes;
- clearer structures and processes: i) organisational restructuring around customer segments; ii) skill-profiled adjustment for digital age;
- resilient and efficient IT backbone: i) a simplified IT landscape; ii) cloud adoption of a certain percentage of platform scope; iii) better data capabilities.

The ECB observed another good practice in this area: a well articulated digital strategy based on a balance between the global vision of the executive leadership and the operational realities of the business units, tailoring the high-level priorities according to the bank’s specific activities, markets, clients and geographical coverage.

- In support of each business line’s strategic plan, there is a central effort to drive different entities towards the definition, monitoring and alignment of the information system strategy, the group strategy and the technological priorities. This allows the monitoring of initiatives delivered in the IT, enterprise architecture, security, data, digital and financial fields.
- Centrally, the institution is building up a digital net banking income metric to ensure alignment with the business strategy and associated financials. This helps evaluate the contribution of digital initiatives to the group’s value generation.

Another aspect of a well articulated digital strategy is detail on the technologies underlying the main digital initiatives. In particular, digital initiatives are linked to the following technological areas of interest: next generation technologies and optimisation of legacy systems; the development of cloud

platforms, and the use of AI for extreme automation. The engineering team is a key stakeholder in the definition of the strategic plan and is also in charge of defining the institution's development of new architectures and innovative applications.

2.3 Execution capabilities

Assessment criterion 3: Does the institution have in place adequate financial and non-financial execution capabilities for the proper implementation of the digital strategy as defined?

Assessment criterion 3.1

Does the institution have in place a clear and robust budgeting process to support the implementation of the digital strategy and its initiatives? Clarity here implies a multi-year budgeting process, aligned with the digital strategy, assigning a level of resources commensurate with the ambition involved in the digital initiatives. Robustness requires a budgeting process specifying both the rationale for budget allocation (for instance expected pay-offs identified through cost-benefit analysis) and the mechanism for budget recalibration or adjustments, if needed.

Assessment criterion 3.2

Does the institution have in place a proper project management framework for steering the implementation of digital strategies? A proper project management framework would typically include an operational plan for executing digital initiatives, detailing timelines, milestones, roles, responsibilities and resources, and aligned with strategic objectives. The structure of such an operational plan makes it possible to gauge interdependencies across projects and to disentangle single digital initiatives, so as to facilitate their monitoring, reporting and follow-up at group level. The evaluation of digitalisation strategies is to consider the investments made.

Box 3

Examples of observed sound practices: execution capabilities

The ECB observed that cross-team collaboration and periodic reviews of the digital strategy help institutions to i) prioritise projects and ii) reconcile the strategic top-down view with the bottom-up and project level view. Sound project management practices include elements such as the following:

- the top-level strategy is translated into business lines and teams collaborate to i) define a plan with the required budget, resources and expected deliverables, and ii) deliver on the plan, flagging adjustments or reprioritisations when needed;
- potential impediments and concerns are raised with the next level in the hierarchy and the escalation continues until the issues are resolved;
- frequent review processes track the progress on delivery and the achievement of the objectives up to the level of the Board of Directors;

- the Board of Directors, in the context of the business plan, flags critical aspects of execution that should be prioritised, progress on the specific roadmaps concerned is directly reported to the Board of Directors and addressing any related backlog is given highest priority.

To provide an additional example, another sound practice observed was the steering of the execution of digital priorities at group level by means of a development agenda. This agenda was aimed at prioritising the allocation of human and economic resources. Resources were assigned to projects according to their impact and strategic alignment. Periodic reviews covered progress in general and on milestones, commitments and deliverables, as well as resources and budget required. There was a quarterly review of the strategic projects portfolio to decide on their prioritisation, monitor their planning and execution, and to challenge initiatives – with potential action points and reallocation of resources and required investments.

Another sound practice observed was the implementation of a new organisational model to drive the execution of digital initiatives: “digital labs”. This involves a network of miniature digital start-ups, each focused on a specific business domain (e.g. personal lending, investments, mortgages, cards or payments). Meanwhile the network retains centralised core competences (e.g. IT, digital business, design and user experience).

To gain speed and agility, each digital lab adopts agile practices and owns a portfolio of initiatives in its specific business domain. Lab initiatives are set out in lab-level operational plans that track deliverables, timelines and milestones (including user acceptance testing and product launching). Dependencies on the initiatives of other labs are also monitored. Each operational plan is accompanied by a summary of the strategic context that anchors the plan in the business strategy-related macro-initiatives and objectives.

Operational plans are dynamic as they can be continuously updated to reflect changes, such as the inclusion of new initiatives, shifts in prioritisation or delays. Adjustments are discussed in monthly lab steering meetings.

To optimise the execution of the digital lab initiatives, a few principles are followed:

- initiatives are categorised according to timeline elasticity;
- effort-cost of execution may exceed the original plan by a set maximum percentage – above this level there is a reassessment of the scope, timeline and capacity allocation for the project;
- when a critical dependency occurs and there is no short-term solution, a decision may be taken to stop the project.

As the digital strategy is embedded in the business strategy, digital initiatives are integrated in the general annual budgeting process. However, the most strategic digital initiatives carried out in the labs are funded by budget pools, achieving agility by allowing for adjustment of allocation and prioritisation.

Finally, another sound practice observed was setting up “ideation labs” for innovation purposes. Such labs are put in place to come up with a long list of potential use cases for new technologies (e.g. AI), selecting the most viable ideas for development.

The development phase employed “user experience” (UX) labs with groups of customers to test each “minimum viable product” (MVP) and adapt feedback on features and functionality to iterate

from MVP1 to MVP2 and so on until the go-live. Such UX labs were also used to test even modest changes to mobile application functionalities.

2.4 Key performance indicator framework

Assessment criterion 4: Is the institution developing a comprehensive framework of financial and non-financial KPIs against which to monitor the implementation and execution of the digital strategy and reassess it if targets are missed?

Assessment criterion 4.1

Is the KPI framework sufficiently comprehensive to allow for the proper implementation of the digital strategy? Does the KPI framework ultimately reflect how the digital strategy is translated into measurable digitally-driven impacts (both financial and non-financial)?

An ideal set of KPIs is i) granular and multi-layered across all levels of the organisation involved in defining the digital strategy and implementing digital projects. The granularity helps reconcile the top-down strategic view with the bottom-up and project level dimensions. Moreover, an ideal framework includes ii) measurable and actionable KPIs, which are used for different levels of reporting, and iii) KPIs with clear ownership and responsibility, which are regularly monitored and reviewed.

Assessment criterion 4.2

Does the institution understand the reasons for missed KPI targets, and incorporate the lessons learnt from failed initiatives into the strategy update? In other words, if critical KPIs linked to the implementation of critical projects are missed, is the institution able to re-scope a project and feed lessons learnt into the reassessment of the strategy? A critical element is the existence of a feedback loop for incorporating those lessons learnt into new strategy development.

Box 4
Examples of observed sound practices: a comprehensive and well-structured KPI framework

In terms of adequacy of the KPI process, the ECB observed that some institutions make use of a solid firm-wide KPI framework that can be easily extended to steer the implementation of the digital strategy and projects. The following are examples demonstrating the adequacy of the KPI process framework.

- Measurement: digital KPIs have a specific measurement methodology documented in a glossary.
- Monitoring: digital KPIs are tracked through an automated system and dashboards. Whenever possible, there is an attempt to include real-time KPIs to be immediately analysed by a dedicated digital team.

- Reporting: digital KPIs are reviewed by all the relevant reporting lines. Reports are structured to provide insights into each KPI, highlighting trends, achievements and areas where deviations from the plan occurred.
- Performance assessment and follow-up: as KPIs track progress on strategic objectives, significant deviations from targets trigger a detailed analysis of underlying factors behind delays/missed targets.
- Decision-making: if critical KPIs are not being reached (e.g. there is a decline in the pace of growth in digital clients), more resources are allocated to the associated project and the operational plans are revised accordingly.
- Granularity: top-layer digital KPIs are defined at business strategy level and are presented to executive management on a quarterly basis; middle-layer KPIs are reported monthly to dedicated committees and cover business dimensions (such as adoption, engagement, sales, change management, etc.); operational KPIs for the relevant business lines are available on the dynamic dashboard and include real-time and next-day metrics to support project execution.
- Communication: KPIs are used not only to report progress to executive committees and the Board of Directors, but also for investors and public disclosure.

Regarding the comprehensiveness of the financial and non-financial KPIs framework, the ECB has observed different approaches.

- Many institutions have in place non-financial KPIs related to customer satisfaction and engagement, the use of digital channels and volumes of digital transactions.
- Some banks have developed a more advanced set of KPIs to monitor the digital strategy. For instance, one institution is implementing a comprehensive end-to-end digitalisation strategy across the most important customer journeys by mobilising the relevant teams, tracking progress, and creating incentives to advance these initiatives throughout the organisation. To this aim the institution has developed, among other things, a group-level “digital index” (target-setting and progress tracking tool), as a summary of digital indices from different geographical areas. The digital index measures the success of digital journeys per segment (e.g. daily banking, lending, or savings) and it is therefore composed of several underlying metrics. Full-time equivalents (FTEs) are allocated and tracked at geographical level, and linked to the digital index.

The ECB also observed a few institutions starting to develop financial KPIs to monitor the profitability impact of their digital strategies and initiatives.

- For instance, one financial KPI is the concept of a digital dividend (both backward and forward-looking). This was structured as follows: first, all digital sales (realised or as targeted in the financial plan) per product line are aggregated, which is the sum of all revenues generated by products sold digitally. Then, on the cost side, maintenance and investment costs (based on invoices or estimates) for each digital project are taken into account.

- In another example, the development of financial KPIs was a tool to ensure alignment between digital initiatives and the financial objectives outlined in the business strategy. To this aim, the institution built: i) a digital net banking income tracker (see also Box 2) to isolate the digital component (e.g. digital sales and income from digital channels) of the overall banking income; and ii) a data/AI value, which measures the expected economic contribution from the use cases for data/AI.

3 Assessment criteria relating to governance

Articles 73 and 74(1) of the CRD, as further specified by the EBA Guidelines on internal governance, require institutions to implement internal governance arrangements, processes and mechanisms to ensure effective and prudent management of the institution.

In accordance with Article 88(1)(a) of the CRD and as specified by the EBA Guidelines on internal governance, the management body must have ultimate and overall responsibility for the institution and defines, oversees and is accountable for the implementation of the governance arrangements within the institution that ensure effective and prudent management of the institution. Furthermore, the management body should fully know and understand the legal, organisational and operational structure of the institution ("know your structure") and ensure that it is in line with its approved business and risk strategy and risk appetite and covered by its RMF. This therefore also includes the digitalisation strategy and digital initiatives.

According to Art 91(1) of the CRD, members of the management body shall at all times be of sufficiently good repute and possess sufficient knowledge, skills and experience to perform their duties. The overall composition of the management body shall reflect an adequately broad range of experiences. The management body shall therefore possess adequate collective knowledge, skills and experience to be able to understand the institution's activities, including the main risks. This therefore also includes the necessary digital knowledge and skills to have an understanding of risks related to digital activities.

The role of non-executive members of the management body within an institution must be carried out in accordance with Article 88(1) of the CRD in conjunction with Article 91(8) of the CRD and in line with recital 57 of the CRD and the EBA Guidelines on internal governance. Accordingly their role should include constructively challenging the strategy of the institution and thereby contributing to its development, scrutinising the performance of management on achieving agreed objectives, satisfying themselves that financial information is accurate and that financial controls and systems of risk management are robust and defensible, scrutinising the design and implementation of the institution's remuneration policy and providing objective views on resources, appointments and standards of conduct. This therefore requires them to challenge management on the digitalisation strategy and ensure relevant risks are covered.

With regard to third-party dependencies, the EBA Guidelines on outsourcing could provide a main reference point. Finally, the requirements under the EU's Digital Operational Resilience Act (DORA), specifically as regards the oversight of critical information and communications technology (ICT) third-party service providers, may apply. Articles 28 to 30 indicate the need for proper oversight and an overview of contracts with critical ICT third-party service providers, information on how the institution addresses potential weaknesses and disruptions, and concentration risk assessment. These articles also state that institutions remain ultimately responsible for compliance with the regulatory requirements stemming from financial legislation.

3.1 Coordination and steering of digital initiatives

Assessment criterion 5: Does the institution have a clear allocation of responsibilities related to digital topics in the management body, whether individual allocation to those within its management function/executives, and/or senior managers reporting to the executive management, or a dedicated centralised steering/coordination body, so as to adequately coordinate digital initiatives at group level?

The central coordination and steering could be assigned to the management body in its management function/executives or delegated to senior managers who directly report to the management body/executives.

Assessment criterion 5.1

Does the institution have central coordination and steering of digital initiatives in the form of a central coordination body, proportionate to the institution's complexity and scope? This can also entail fully embedding digitalisation in the steering of the organisation. A central coordination body assists the whole management body in its management function with the implementation of the digital strategy, by ensuring that the Board of Directors has the right information to develop and monitor the overall digital strategy.

Assessment criterion 5.2

Does the central steering include, as a minimum, a clear and focused approach to the following aspects:

1. alignment of digitalisation projects across the organisation, including the subsidiaries;
2. strategic alignment, with a focus on aligning business and IT strategies;
3. staff and resource management, to ensure sufficient expertise for the roll-out and execution of the strategy;
4. sound reporting to the management body in its management function/at executive level on the digitalisation strategy and related projects and progress made?

Box 5

Examples of observed sound practices: dedicated units responsible for the digitalisation strategy

The ECB observed institutions with a dedicated team or department responsible for coordinating and steering as well as executing the digitalisation strategy and digital projects. The team or department was either within the management body or directly reporting to the management body, with clear responsibilities set also at the executive level. The coordinating unit was responsible for the roll-out of the strategy at group level and ensuring consistency between the group entities and business lines. This was facilitated by clear ownership of the digitalisation activities at all levels of the organisation in order to foster the coordination of digital activities at group level both bottom-up and top-down. This was further supported by adequate governance at the level of the regional groups and for the various business lines, in order to further roll out the strategy.

More specifically, the ECB observed those units as having responsibility for the following:

- Strategic alignment, with a focus on aligning business and IT strategies and/or the digital strategy specifically, in order to make sure that digitalisation aspects are consistently addressed.
- Alignment of the digitalisation projects across the organisation, including the subsidiaries, by discussing projects undertaken, their main objectives and benefits, and how synergies between various projects could be achieved. This also helps prioritise projects and equip central expertise centres with mandates to define and roll out digital projects throughout the organisation in a consistent manner.
- Identification and management of interdependencies by means of detailed roadmaps, e.g. when some projects are enablers of others and certain milestones need to be achieved in order to allow a dependent project to move on to the next task/milestone.
- Staff and resource management, to ensure sufficient expertise for the roll-out of the strategy in line with the prioritisation. In this context central expertise centres can also help address any shortage of staff, although it needs to be ensured that the specific needs of local/regional subsidiaries are also sufficiently addressed, and that there is relevant expertise at regional/business line level.
- Workforce planning, recognising different needs at different phases of the roll-out to feed the information into hiring (including external developers), training and reskilling plans.
- Sound reporting to the management body in its management function/at executive level on the projects undertaken, their progress and any potential risks that may need to be addressed (e.g. in terms of execution).

The ECB also observed some institutions where digitalisation was completely embedded in the overall strategy and organisation, with attention to digitalisation coordination, steering and reporting in all relevant areas and aspects.

3.2 Monitoring and reporting

Assessment criterion 6: Does the institution set up adequate monitoring processes (top-down), and define the business areas ultimately responsible for reporting on digitalisation initiatives, as well as establishing a proper reporting process (bottom-up), covering all subsidiaries and business lines?

The central coordination body is responsible for the monitoring and needs to define relevant business lines to report on the progress made.

Assessment criterion 6.1

Does the institution have in place adequate monitoring processes related to its digital strategy and, accordingly, an adequate process for reporting to the management body in its management function/at executive level with regard to digital topics? This involves defining the business area(s) ultimately responsible for the reporting. Such reporting encompasses the main findings, issues for discussion and the central body's advice to the management body in its management function/at executive level.

If the institution has in place a suitable structured process, it will be able to adequately monitor the roll-out and execution of the digitalisation strategy and take actions and escalation measures in case KPIs are not met.

Assessment criterion 6.2

Does the institution effectively monitor the digitalisation strategy? The institution:

1. devotes sufficient time to digital topics during meetings of the management body (for both the management and the supervisory function), allowing discussion on the strategy, progress of various projects and related risks;
2. has in place adequate top-down and bottom-up monitoring processes related to its digital strategy, also sufficiently covering its subsidiaries and various business lines;
3. has set up an adequate reporting process indicating progress and relevant challenges and risks that need to be discussed, with a clear escalation process.

Box 6
Examples of observed sound practices: digital transformation initiatives translated into operational plans

The ECB observed institutions with digital transformation initiatives translated into operational plans including timelines, milestones, and associated information such as objectives, roles and responsibilities. These plans were further consolidated into the overall operational plan for digitalisation in order to enhance monitoring of digital progress. Subsequent waves of innovation trigger updates on the structure for decision-making and challenging, KPIs and reporting lines.

Some institutions impose regular monitoring meetings to discuss operational plans for digital initiatives, KPIs, adjustments or delays. In particular, challenges and risks related to digitalisation are reported to the management body on a regular basis, e.g. monthly. Sometimes, a second line view on the projects and their assessment was presented as part of the risk map. The

coordination/steering body can take decisions based on the monitoring information on the steering, alignment and prioritisation of the digital initiatives.

More specifically, the ECB observed institutions that ensure the following.

- Sufficient time is devoted to digital topics during meetings of its management body in its management/executive function to allow discussion on the strategy and related risks, by having a specific time slot reserved, e.g. once a month, at which various project owners are present.
- The allocation of adequate human, financial and technical resources is discussed in relation to the strategic objectives, based on the progress monitoring reports.
- The institution has in place an adequate processes for the implementation of the top-down steering as well as bottom-up monitoring related to its digital strategy, taking project risks into consideration. Some banks for example have monthly meetings with an increase in frequency according to the status of individual project (red, amber or green).

3.3 The management body in its supervisory function/non-executives' capacity to challenge

Assessment criterion 7: Does the institution have a management body with a supervisory function/at non-executive level that constructively challenges the management body in its management function/at executive level and that provides effective oversight for the digitalisation strategy and related risks?

The management body in its supervisory function/at non-executive level (management board supervisory function; MBSF) also oversees and challenges the digitalisation initiatives.

Assessment criterion 7.1

Does the institution have an MBSF which constructively challenges the management body in its management function/executives (management board management function; MBMF) and provides effective oversight of the MBMF, also in the context of digital topics and their related risks? The MBSF should proactively discuss and bring to the agenda digitalisation-related topics.

Box 7

Examples of observed sound practices: the MBSF has a clear role in challenging the MBMF

The ECB observed institutions where the MBSF selected the topics to be discussed with the MBMF/executives in order to assess the digitalisation strategy, request updates on the progress of the main digital projects as well as review new product approval procedures. This could also involve reviewing the evolution of the training of MBMF/executives on digital transformation.

In addition to the agenda put forward by the MBSF, some banks also organise a dedicated Q&A session between the MBSF and MBMF on digitalisation, for example on a bi-monthly basis.

The ECB also observed that most banks have a specific digital committee at MBSF level.

3.4 Internal control functions' involvement in decision-making on digitalisation

Assessment criterion 8: Does the institution provide internal control functions with a strong role in the digitalisation strategy process, the NPAP and ongoing business operations, while ensuring their independence?

It is a sound practice for Internal Control Functions (ICFs) to be involved in approving the digitalisation strategy, new products or significant changes to existing products, processes and systems as well as ongoing risk assessments, in order to also include the impact of digitalisation-related risks.

Assessment criterion 8.1

Does the institution ensure that ICFs have a strong role in the strategy process and new product approval/review processes, as well as ongoing business operations, in order to take into account risk dimensions in digitalisation-related decision-making, while fully respecting the independence of the ICFs?

In particular, it is sound practice for the compliance function and risk management function to be involved in approving the digitalisation strategy, new products or significant changes to existing products, processes and systems, according to their respective mandates.

Assessment criterion 8.2

Does the institution carry out a full and objective assessment of the risks arising from new activities under a variety of scenarios, and of the ability of the institution to manage and control any new risks effectively?

ICFs need direct access and/or to report directly to the management body (both its management and its supervisory function). The management body needs to be kept properly informed by the ICFs, and receive reports on any major deficiencies and risks identified in relation to digitalisation, with recommendations and corrective measures to be taken.

Box 8
Examples of observed sound practices: involvement of the ICFs in the digitalisation strategy

The ECB observed institutions where the risk dimension is an integral part of the digitalisation strategy-setting and of any decision to change the strategy, the new product approval procedures for digital products or services and the monitoring of digital activities. This includes the ICFs already having a strong role in the digital strategy-setting phase, sometimes with a veto or decision-making power. For some institutions, more specifically, the chief risk officer (CRO) is part of the strategy-setting phase and ICFs are involved in all phases of the design and roll-out of the digitalisation strategy.

At a few banks, a dedicated risk workstream complemented business line and operational workstreams in the strategy-setting process and conducted a holistic risk assessment of the digital strategy towards the end of the process. The compliance function supported this by identifying specific regulatory issues which could – and eventually did – cause delays.

The ECB has also observed banks which specifically mention digitalisation topics in their reporting to the MBSF from the ICFs, or in special digitalisation risk reports that are submitted to the decision-making bodies at a pre-defined frequency. Here the information is shared both bottom-up and also top-down, as the management body subsequently reports back to the ICFs on the decisions taken.

3.5 Digitalisation risk culture

Assessment criterion 9: Does the institution embed digitalisation in its risk culture (e.g. tone from the top, incentives, risk accountability, culture of challenge) both top-down and bottom-up, including the communication on strategy and risks, creating awareness and fostering knowledge?

Assessment criterion 9.1

Does the institution's management body foster a risk culture which also includes technological advancements within the organisation? The following are indicators of fostering an appropriate risk culture.

1. The institution ensures regular communication and proper coordination between all staff involved in delivering the digital transformation strategy, including project managers, ICFs, business analysts, support functions and the business areas affected, in order to discuss and obtain feedback on issues important to its successful execution.

2. It ensures that a culture of effective communication and challenge exists at all levels, especially within the management body, its committees, ICFs and business lines, and with respect to all types of risks. It ensures accountability for risks including digital ones in relation to monitoring, managing and mitigating those risks. This encourages collaboration, communication and the opportunity for staff to challenge the digital transformation initiatives. This in turn ensures consistency and the existence of safeguards, as well as prudent risk-taking, without impacting the independence of the ICFs.

To achieve this, institutions ensure full alignment of behaviours within the different units of the organisation – clear and open communication on decision-making processes as well as a "culture of challenge" are of utmost importance.

Assessment criterion 9.2

Does the institution make sure that the financial and non-financial incentives of people working on digitalisation also take into account the implications of digitalisation developments on the internal controls of the bank?

Box 9

Examples of observed sound practices: dedicated programmes to promote digital risk culture

The ECB observed institutions with specific teams or innovation labs to test and roll out digital projects or ideas. This could also foster the use of innovative technologies by employees. Examples are the testing and use of, for example, a chatbot for internal use or a specific AI application for administrative purposes. This helps employees engage with innovative technologies and better understand the capabilities and potential risks also from first-hand experience.

Some institutions have dedicated programmes designed to nurture internal innovation. Through these programmes, every employee has the opportunity to showcase their innovative ideas and solutions. Examples are challenges and contests where employees can present their initiatives, creating a culture of innovation and engagement, and which also raise awareness of risks. Another example might be hackathons that offer employees a dedicated period to dive deeper into problem-solving on a specific opportunity, e.g. a new customer experience or back-end optimisation. Typically, the best winning ideas get a chance to be implemented in innovation labs or development hubs. The experience with innovative technologies is also intended to enhance awareness of risks related to data input and output, bias, etc.

Cross-cutting governance committees chaired by the chief executive officer (CEO) and with members from various levels and business units also foster innovation throughout the organisation. This was seen specifically in some cases where the institution involved staff from all layers of the organisation in further spreading the innovation agenda and rolling out innovations in their business areas. This also prevents a silo approach and ensures accountability.

3.6 Assessment of critical dependencies

Assessment criterion 10: Does the institution ensure insight into and monitoring of critical dependencies, interdependencies and third-party relationships, and not only of outsourcing, on an ongoing basis?

Assessment criterion 10.1

Does the institution ensure the monitoring of critical dependencies, interdependencies and third-party relationships on an ongoing basis? This would encompass the following activities:

1. The institution has a policy in place for identifying critical dependencies on procedures, software and third-party risk management (and not only for outsourcing).
2. It ensures that the internal audit function has access to third-party agreements, as well as access and cooperation arrangements between the internal audit function and the third-party within the sourcing strategy.
3. The institution is aware of the ownership of the key innovative technology developed within the third-party relationship.

4. It assesses the interconnections between different providers and the impact on the value chain.

5. It defines a risk tolerance scope for risks related to third parties.

6. In its first analysis of the relationship, the institution considers the grey area where third-party relationships do not necessarily constitute outsourcing based on the EBA Guidelines, but are nonetheless critical dependencies including critical ICT service providers as defined by DORA. Even if not classified as outsourcing, these relationships are adequately assessed in terms of dependencies and interdependencies. They are also managed and monitored to enable dependency quantification and, to identify concentration at institution level as well as across the supply chain, taking into account the DORA requirements.

7. The institution assesses the need for a realistic and feasible exit plan.

Box 10

Examples of observed sound practices: high-level sourcing strategy and adequate controls

The ECB observed institutions with a high-level sourcing strategy for all the material technology applications and projects. In addition, some institutions have a detailed overview with a mapping of all third-party service providers. For a few banks these providers have also already been assessed and ranked based on their criticality and importance, for example based on relevance for front and back office operations or customer relations.

Some banks have in place adequate controls and appropriate oversight measures to ensure that the processes outsourced or otherwise handled by third-party providers are aligned with the risk profile of the bank and its self-assessment of the risk level. The ECB also observed other sound practices for fostering adequate control in this area, such as:

- performing the risk assessment before entering into any new relationship and reviewing it at pre-determined intervals;
- formalising a strategy approved by the management body that describes in detail the scope of the use of external partners, also beyond the scope of outsourcing;
- conducting a regular follow-up on dependencies on key providers also including interdependencies between suppliers.

Finally, the ECB observed some banks assessing the impact on the risk profile and keeping track of the impact on compliance aspects.

4 Assessment criteria relating to risk management

Article 74(1) of the CRD requires institutions to have robust governance arrangements in place. These include: a clear organisational structure with well defined, transparent and consistent lines of responsibility; effective processes to identify, manage, monitor and report the risks they are or might be exposed to; adequate internal control mechanisms, including sound administration and accounting procedures; and remuneration policies and practices that are consistent with and promote sound and effective risk management. This requirement therefore also includes digitalisation-related risks, and an assessment of how digitalisation is impacting the risk profile.

Article 76(1) of the CRD provides that the management body is to approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks the institution is or might be exposed to, among other things. Such policies and processes in respect of digitalisation activities and related risks, also including all relevant financial and non-financial risks, are to cover the identification, management, monitoring and mitigation of those risks.

4.1 Risk identification

Assessment criterion 11: Does the institution run a detailed impact review of traditional and non-traditional risk dimensions during the digital strategy-setting process and the NPAP as well as during the execution of its digital strategy?

Assessment criterion 11.1

Does the institution run a detailed impact review of all financial and non-financial risk dimensions during the digitalisation strategy-setting and execution process (including credit, liquidity, market and operational risks, anti-money laundering (AML)/fraud governance, reputational impact and capital impact) covering risks arising from digitalisation? This is a comprehensive process not restricted to IT/cyber risk and operational risks.

A similar assessment should be performed as part of the NPAP and when there are amendments to the digitalisation strategy.

Box 11

Examples of observed sound practices: identification processes of risks related to digitalisation

The ECB has observed banks running an assessment of all financial and non-financial risks such as credit, market, operational and reputational risks as well as capital and liquidity impact, with a detailed overview of how these could be affected by digitalisation.

The ECB observed banks with specific processes – in line with the general procedures above – to identify and assess new risks (i.e. risks that the bank does not already consider) arising from digitalisation and the implementation of innovative technologies: AI, cloud computing, distributed ledger technologies (DLT) and application programming interfaces (APIs). The ECB has observed

some detailed risk maps and overviews indicating, for each risk area, how it could be affected by the digital strategy. The same is done for the launch of new digital products and services.

One bank's multi-year financial planning considered an idiosyncratic adverse scenario in which the risks of its digital transformation strategy "going wrong" were identified: (i) employees (high levels of uncertainty may lead to human resource risks and attrition); (ii) postponement of IT architecture modernisation and implementation of new digital features (leading to higher costs); (iii) consequent operational instability, combined with pricing measures and dissatisfaction with the new support model, might lead to loss of reputation, earnings and customers. The total impact of this adverse scenario was presented for each of stage of the plan, also drilling down to identify which business lines would be most affected.

Some banks also closely involve the second and third lines of defence in order to cover all risks related to digitalisation. The ECB has observed a sound practice whereby the NPAP covering new digital services requires a specific opinion and authorisation from the AML function.

4.2 Data governance framework

Assessment criterion 12: Does the institution have in place a data governance process to support data-driven digitalisation initiatives?

This includes a review of the availability of data relevant for digitalisation and for supporting such activities.

Assessment criterion 12.1

Are the sound data governance practices as set out in Chapter 3.2 of the ECB Guide on effective risk data aggregation and risk reporting applied for data-driven digital activities, as well as data generated by digital means? Are they are applied based on criteria as identified by the bank taking into consideration its digitalisation strategy and the nature, scale, complexity and risk profile of its operations? **More specifically, do institutions have in place a data governance framework to support data-driven digitalisation activities with clearly defined roles and responsibilities?** This data governance framework defines, among other things, the responsibilities of data owners, and the policies and processes for data lineage and independent validation to ensure availability and quality of the data within the data governance framework as defined by the bank. In this regard the bank reviews the availability of data to **measure digitalisation and related risks**, and to be able to produce timely and accurate reporting to the Board of Directors, also independently of the relevant business area, which is the first line of defence.

Assessment criterion 12.2

Are the digitalisation plans aligned with the bank's ability to maintain, capture, and exploit data both resulting from digital activities and benefiting them? Do its digitalisation strategies consider the impact on risk aggregation capabilities, **also in light of already existing risk data and reporting (RDAR) weaknesses?**

Box 12

Examples of observed sound practices: data governance framework in line with digitalisation initiatives

The ECB observed banks increasingly updating their data governance frameworks to foster data-driven decisions also with respect to digitalisation initiatives. In particular some banks have:

- a data governance framework that includes all the entity's relevant data, regardless of their origin, including digital-driven data or data relevant for digital initiatives;
- a unified governance structure and single data lake containing all of the bank's data with appropriate data quality controls, in turn facilitating all reporting, modelling and a full customer 360 degree view for analytics-driven sales;
- an extensive data management framework also covering "new" risk dimensions/risk maps;
- automated data quality checks for the detection, correction and removal of data inaccuracies/inconsistencies;
- a dedicated data quality KRI dashboard reported to and actively discussed in the management body with appropriate follow-up;
- root cause and impact analysis of data quality issues to drive improvements within defined timelines;
- specific attention to the identification and reporting of risks coming from innovative technologies (e.g. AI or APIs);
- special attention for change projects, including digital ones, and their impact on risk data aggregation capabilities;
- checks against record requirements for any new application, any change in application, any application migrating to the cloud and any new central data sharing, with cataloguing of data class and data flows.

Furthermore, the ECB observed one example where the data office was part of the digital office in order to ensure synergies.

4.3 Risk modelling

Assessment criterion 13: Does the institution assess and update the risk map and relevant risk metrics in all risk dimensions, and review and adapt the suitability of existing risk models in view of digitalisation?

Assessment criterion 13.1

Does the institution assess and update the risk map and relevant risk metrics to reflect changes in all potentially relevant risk dimensions (for example business model, liquidity, credit risk, operational risk, market risk, IRRBB, governance, AML/Fraud)? Does the institution review and potentially adapt the

suitability of existing risk models – including interest rate in the banking book (IRBB), early warning systems (EWS), stress tests and scoring models – related to changed customer behaviours or shifts in business processes in response to digitalisation and the use of innovative technologies?

Box 13

Examples of observed sound practices: risk mapping and modelling for new technologies

The ECB observed sound practices such as a new risk map of risk metrics related to digitalisation. These maps evolve in order to incorporate new challenges and initiatives but also new risk assessment conclusions. Specific metrics could be defined for example for AI or third-party reliance. These maps include a definition of qualitative risk tolerance and the identification of suitable metrics, in order to mitigate risks related to technology innovation and use of new technologies.

One example is the development of new credit risk models across the credit risk lifecycle. This takes into account digital channels using credit risk models with specific customer and digital sales information for digital channels and business/subsidiaries. These could be fed with specific data sources from digital channels. Also, digital parameters (e.g. digital as opposed to physical branches) as a risk driver for capital calculations are explored.

Further metrics observed are related to IT and digital transformation risk, digital assets and to monitor specific risks e.g. in relation to AI.

Some banks have also been identifying new credit risk models for origination in the open market (acquisition scorecards, behavioural scores for pre-approved limits and income estimation models) and have assigned a specific capital add-on as a result of the change in the risk mapping. The ECB also observed new institutions where new products/instruments cannot be introduced without model validation function confirming ex ante that any impact on existing models has been validated.

At one institution, an indicator framework allowing early detection of social media threats, media tonality, etc. has been introduced. Such early warning indicators are closely monitored and linked to the crisis governance framework. For some institutions, developing various threat scenarios helps identify specific risks.

4.4 Update of the RAF, the RMF and KRIs

Assessment criterion 14.1

Do institutions review the RAF, RMF and KRIs defined ex ante to ensure they adequately cover digitalisation-related risks? Do they adapt them if needed, for example by defining suitable KRIs to capture new or altered risks related to digitalisation (if the risk is measurable)? Both quantitative and qualitative indicators can be used in the RAF to sufficiently cover risks which are not easily measurable, such as non-financial risks including digitalisation/IT-related risks. The institution reviews and, if necessary, updates existing KRIs to capture a change in sensitivity related to digitalisation. This also includes the definition of “red flags” or ‘early warnings’, i.e. thresholds that trigger decisions on mitigating measures.

Box 14

Examples of observed sound practices: processes designed to update the RAF, RMF and KRIs

The ECB observed institutions considering the need to update their RAF and RMF in view of the impact of digitalisation, and in order to add new digital-related metrics and review risk tolerance. The ECB also observed banks including digital metrics in the RAF and reviewing them on a regular (e.g. annual) basis. The review included changes in the risk tolerance (e.g. related to economic capital and exposures to consumer-related credit risk), mostly in relation to changes in the digital environment and cyber threats with implications for the digitalisation of processes, services and products. The ECB observed banks setting thresholds for specific risks, e.g. percentage of critical applications run on external services as a threshold for third-party risk.

With regard to KRIs, the ECB has observed sound practices at some banks on the implementation of KRIs. These practices involve measuring risks affected by digitalisation in parallel with the risk identification process (business continuity, vulnerabilities, critical service providers, cyber controls, AML and fraud). Another sound practice links these KRIs, for example, to digital customers, application activities, or the percentage of systems operating in the cloud. Best practice is to also align the KRI development process with any necessary update of the RAF/RMF.

In the context of the digital risk framework, the ECB observed institutions where:

- KRIs are developed in the context of digital initiatives, and their outcome fuels other supervisory exercises if needed (especially the RAF);
- IT/third-party risks are included in the RAF based on newly added metrics and adjusted risk tolerance and consumer credit/distribution channels;
- transformation dashboards are included and updated in the RAF/RMF.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

PDF ISBN 978-92-899-6789-1, doi:10.2866/681424 QB-05-24-468-EN-N
HTML ISBN 978-92-899-6788-4, doi:10.2866/136159 QB-05-24-468-EN-Q