

# CAPCO

THE FUTURE REDEFINED

---

CAPCO

---

# INTRODUCTION

---

Institutions are looking for new perspectives and innovative approaches as they navigate towards a post-COVID new normal. Drawing upon our substantial library of published thought leadership, we have curated a select number of articles that explore the key themes, challenges and opportunities for our clients and the wider global financial services industry.

---

## OPERATIONAL RESILIENCE

Operational resilience is central as institutions prepare for an ever-changing world. Our thought leadership selection on this topic can help your organization plan for uncertainty, better manage change and address crisis scenarios. We look at the OODA Loop (observe, orient, decide, act) checklist - a military approach that firms can incorporate into Business Continuity Planning to assist better and faster decision making. We also assess the challenges around meeting the UK operational resilience regulation.

- [Managing the inevitable: A primer on operational resilience](#)
- [Getting ready: Challenges to meeting the UK operational resilience regulation](#)

---

## NEW WORKING PARADIGMS

Financial institutions have an unprecedented opportunity to strategically transform their workforce and operations. The pandemic has made many firms realize that they were better prepared for digitalization than previously thought. We look at how firms can draw on their lockdown experiences to embrace new ways of working and refresh their digital strategy accordingly. These provisions will help organizations improve productivity, cost effectiveness and employee engagement, whilst enhancing resilience and creating positive customer experience outcomes.

- [COVID-19: Embracing better ways of working in the new normal](#)
- [How to refresh your digital strategy to prepare for the new normal](#)

---

## TECHNOLOGY COST MANAGEMENT & OPTIMIZATION

CIOs have played a critical role in managing the COVID crisis to ensure continuity of business activities. Post-pandemic, they will need to invest smarter and more cheaply and to respond to changes – positive or negative – swiftly and efficiently. We explore how today’s banking CIO can implement a more flexible approach to technology spend management and optimization that will enhance their investment capacity, increase cost transparency, and improve performance and business value.

- Achieving more with less: Technology spend priorities of a post-pandemic CIO

---

## HYBRID, NEARSHORE & OFFSHORE WORKING MODELS

As organizations look to reintegrate workforces post-COVID, there is a clear recognition that alternative working models have proved effective from a productivity perspective and offer the potential for cost savings, amongst other benefits. We compare onsite, remote, nearshore and offshore working models and outline why a hybrid model combining all four options is the most effective approach.

- Hybrid, nearshore and offshore – choosing the correct post-COVID working model

---

## CYBERSECURITY

Cybersecurity is increasingly a critical component in firms’ enterprise risk management frameworks, as they look to design the right capabilities to manage risk, address cyber threats and improve their crisis management response. We consider the expectations of stakeholders – Board, customers, regulators, third parties – when implementing a cyber program, and how to design such programs to ensure continued success. We also highlight the top cybersecurity trends based on our own client projects in 2020.

- Cyber program design and compliance review
- Five cybersecurity trends in 2020

---

We hope that this selection of relevant thought leadership publications will inform your future strategic decisions, helping you and your organization to adapt to the new reality, to benefit from new technologies across all aspects of the enterprise and customer servicing, and to profit from new ways of working.

---

# THIS ISSUE

---

6 | Managing the inevitable: A primer on operational resilience

18 | Getting ready: Challenges to meeting the UK operational resilience regulation

25 | COVID-19: Embracing better ways of working in the new normal

31 | How to refresh your digital strategy to prepare for the new normal



37 | Achieving more with less: Technology spend priorities of a post-pandemic CIO

43 | Hybrid, nearshore and offshore: Choosing the correct post-COVID working model

60 | Cyber program design and compliance review

67 | Five cybersecurity trends in 2020

---



# OPERATIONAL RESILIENCE

---

# MANAGING THE INEVITABLE: A PRIMER ON OPERATIONAL RESILIENCE

---

**AUTHORS:**

Will Packard, UK  
James Arnett, APAC  
Owen Jelf, UK

In recent years ‘expect the unexpected’ has become something of a mantra for a great many of us. Yet, when viewed retrospectively, many of the events we have experienced or witnessed have come to possess an aura of inevitability – whether large scale cyberattacks, data outages, supplier process failures, disrupted commutes, terror incidents, extreme weather events or even pandemics. And while there is typically nothing that links these occurrences, they have all to varying degrees disrupted the ability of financial services firms globally to provide their customers with the expected level of service and support.

The financial ecosystem is becoming ever more complex due to greater outsourcing, wider adoption of cloud computing and the emergence of fintechs across more points within the value chain. All increase the potential for disruption to services; at the same time, firms must cope with enhanced expectations from customers and regulators alike.

Operational resilience is a critical factor to managing these pressures effectively. The underlying assumption behind operational resilience is that events will occur and that firms need to prepare accordingly. It is no longer a question of ‘if’ but ‘when’.

Regulators globally are focusing on this area with renewed intensity given the disruption caused by COVID-19, with the UK regulators taking a lead. The UK’s Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) are looking to roll out regulation in early 2021 that will raise the bar in terms of the approach that firms are expected to take to ensure that

they are resilient. Other regulators around the world will be looking on with interest to see what might be learnt from the UK experience and to replicate or adapt the beneficial elements to their own jurisdictions.

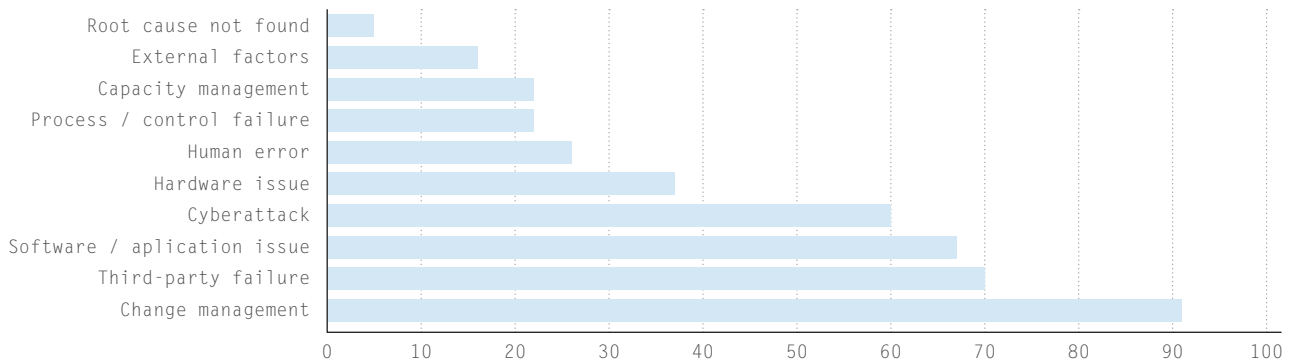
We view the UK regulators’ approach as logical, coherent and – in all likelihood – the model that will come to be adopted globally. For this reason, it is worth reviewing the key proposals within their consultation papers in more detail.

The definition of ‘operational resilience’<sup>1</sup> used by UK regulators is:

**‘The ability to prevent, adapt, respond to, recover and learn from disruptions to better serve customers and, more broadly, ensure financial stability.’**

This well describes the end-to-end nature of the topic well as well as bringing out that it is a process with no defined end state; as the threat evolves so do the responses of firms. The regulators are focusing on the approach that is taken and how seriously the topic is taken.

It is not operational risk. It is about managing the response to a situation that has already happened and not about the likelihood of an event and quantifying the resulting financial impact. It is focused on the broad impact on customers and financial stability rather than the more horizontal/internal focus of Business Continuity Planning (BCP) and Operational Continuity in Resolution (OCIR).



Overview of technology outages report to the FCA (2017 – 2018)

**Source:** Financial Conduct Authority. “Cyber and technology resilience: themes from cross-sector survey 2017 – 2018”, November 2018

Operational resilience should not be seen as a one-off exercise but rather a consideration that should be embedded in how a firm operates, and in all decision-making. The analysis needs to be refreshed regularly and the response to potential events rehearsed on a frequent basis. It is for this reason that UK regulators are requiring annual sign off from legal entity boards on the operational resilience of their firms.

It would also be wrong to assume that operational resilience revolves primarily around cyber threats; most service disruptions are caused by internal errors such as the issues around the TSB data migration in 2018 following its sale from Lloyds to Sabadell<sup>2</sup>. The figure above shows the number of disruptions reported to the FCA in 2017 and 2018 by type.

In the UK responsibility for a firm’s resilience framework rests under the UK Senior Managers and Certification Regime (SM&CR) with the SMF24 Chief Operations Function, the ultimate responsibility lies with legal entity boards or branch management committees. They should be familiar with and sign off the approach as part of the annual self-certification process.

For most firms, many of the elements required to ensure operational resilience already exist to some degree. What has changed is that UK financial regulators have, following an extensive consultation exercise, defined the steps that they expect firms they regulate to undertake ‘to ensure that they are resilient’ Operations is specific to back office functions in many banks. For example operational risk is not the same as operations risk.

Both the UK FCA and PRA published final consultation papers on the topic in December 2019, stating that they expect to publish formal regulations mandating these steps in late 2020/

early 2021 implementation over the following three years. While the principle of proportionality will apply, this is more evident in the sense of urgency expected and the impact tolerances placed on a firm’s business operations rather than omitting any element.

With the PRA focused on financial stability and the soundness of firms and the FCA concerns centered on harm to clients the latter will typically result in a lower impact tolerance.

Both papers<sup>3,4</sup> adopt the same approach in terms of the steps that they expect regulated firms to take. We detail these steps in this paper as they represent a logical approach and will, in all likelihood, be the ones that will need to be undertaken.

The regulators expect more systemically important and complex firms to have completed preparations considerably sooner. There is also undoubtedly a competitive advantage in adopting this approach to operational resilience ahead of peers in being able to demonstrably better serve customers. If they themselves are regulated they will also be looking for the outcome of their suppliers’ self-assessments as part of their own operational resilience preparations in advance of the deadline.

There will also inevitably come a point, ahead of the deadline, that the new standard becomes the market expectation with negative consequences for those firms who have not yet adopted this approach to operational resilience. In addition, service disruptions cost significant amounts of value both in terms of direct compensation and potential fines and, more importantly, the impact on customer trust. This is all on top of just building a better business for the sake of it. It makes sense to be ahead of the pack.

## OPERATIONAL RESILIENCE: A COHERENT APPROACH

THERE ARE THREE DISTINCT PHASES TO  
OPERATIONAL RESILIENCE:

### **Preparing for the inevitable**

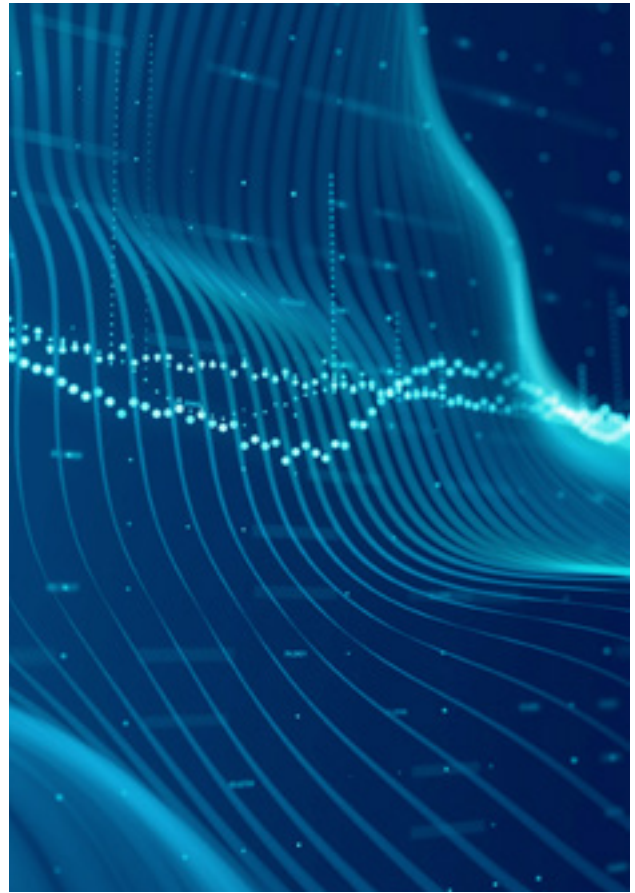
This drives the bulk of the task and involves really understanding the underlying dynamics of key business processes, their vulnerabilities and then testing how they respond to simulated events. The step by step approach taken by the regulators breaks this down into a logical series of actions.

### **Managing the response**

The success or otherwise in responding to an event will be determined by the thoroughness of the steps taken beforehand around training, governance, communications and setting up the physical/informational arrangements to manage the response.

### **Learning lessons**

Processes and procedures need to be reviewed in light of events that have impacted the firm or other organizations to ensure that the approach to resilience is still sound and that the firm can stay within its impact tolerances.





## PREPARING FOR THE INEVITABLE

### IDENTIFICATION OF IMPORTANT BUSINESS SERVICES

The starting point is identifying the important business services which a firm delivers to its customers and, by extension in some circumstances, the market. These are specific, viewed from a customer perspective and include items like making an annuity payment, making correspondent banking payments, providing account balances, selling or buying equities, renewing an insurance policy and the suchlike. They are not internal systems such as a general ledger, HR database or business lines such as mortgages or foreign exchange, nor are they internal systems such as the HR salary system.

“

*They who defend everything,  
defend nothing.*

”

Frederick the Great

### DEFINITION OF IMPACT TOLERANCES

For each important business service, a measurable level of disruption should be defined within firms as the maximum that is tolerable to customers who use the service. The Impact tolerances should be in terms of the impact on clients and also the broader market, if relevant. Impact tolerances should take into account relevant factors such as the number of customers affected and financial loss to them, duration of the disruption, data integrity, substitutability, time of day, impact on market stability, etc.

Once defined, it is the impact tolerance for each of these services that sets the limit that management must take steps to ensure is not exceeded. Remaining within impact tolerances will be the key measure by which the success of a firm’s approach to resilience is measured. This will have the effect of focusing senior managers and boards on the steps necessary to ensure that firms

meet the regulations such as prioritizing spend on changes to IT infrastructure. Firms regulated by both the FCA and PRA may have different impact tolerances due to the need to meet the focus of each regulator.

### MAPPING

To be able to understand the potential points of disruption to a process it first needs to be mapped. Parameters such as timing should be added to the information flows between the components of the processes that deliver all a firm’s important business services. There is a careful balance to be drawn between going into too greater detail and capturing the points in a process that potentially could cause disruption. There is no need to include the mapping documentation into the annual self-certification.

### THIRD-PARTY SERVICE PROVIDERS

With the developments in the provision of financial services and how financial companies are structured leading to increased use of suppliers in key processes, e.g. FMIs, fintechs, cloud computing, there is a growing recognition that resilience extends beyond the traditional boundaries of a firm. There is also an awareness that the provision of services to the market by a limited number of suppliers may itself create concentration risk. To address this, the EBA is recommending the creation of a ‘register of outsourcing’<sup>5</sup> for each firm that, while not necessarily public should be readily available to regulators and stakeholders and include, for critical or important services, detailed information on suppliers. Firms need to be satisfied that their suppliers have put in place appropriate steps to ensure that they can continue to deliver the service they provide in light of disruption. It is expected that this will take the form of reviewing a firm’s operational resilience self-assessment where the supplier is a regulated firm. Where the firm is not regulated a similar level of rigor should be expected.

### VULNERABILITY ASSESSMENT

With the key elements of a process mapped and third parties identified, a thorough review of the vulnerabilities at each step of the process can be undertaken. Some of these will be more general than others (terrorist attack or natural disaster versus EUC host platform failure). All aspects should be taken into

## PREPARING FOR THE INEVITABLE CONTINUED

account, not just technology but also factors such as dependency on key individuals and single points of failure. A good example<sup>6</sup> is the crypto exchange CEO who died along with his passwords.

### VULNERABILITY REMEDIATION

Once vulnerabilities have been identified then the necessary resources should be put against removing each one to the point at that the process can be managed so as to not exceed the defined impact tolerance if an event occurs. This may lead to the acceleration of system replacement as the cost of addressing specific vulnerabilities is uneconomic compared with that of simply replacing legacy architecture. This is also an opportunity to simplify systems into a more customer centric model that is better suited to a world of APIs and increasing integration with suppliers.

The opportunity should also be taken to improve the MIS that is generated on a firm's process performance and status. Once the approach to resilience is embedded it can be designed into systems from inception at little additional cost. Embedding resilience will also involve training individuals responsible for process design and implementation to ensure that good practice is followed and reduce the need for subsequent remediation.

### SCENARIO TESTING

To ensure that impact tolerances are not exceeded given an event a number of plausible scenarios should be run through rigorously to identify each one's impact on the important business services.

While the regulators will not specify the scenarios that should be considered, their emphasis is both on plausible as well as severe events; they fully realize that there are some theoretically possible scenarios or combination of scenarios would cause an impact tolerance to be breached. Scenario testing should be a part of the annual self-certification process.

### SELF-ASSESSMENT

The relevant senior managers and the board should sign off that their firm can remain within its impact tolerances given disruption to its processes, detailing the important business services, the relevant impact tolerances, third-party dependencies as well as the results from the scenario testing. There is no need to describe the processes and mapping in detail. It should, however, talk to the reasoning behind the assessment that the firm is operationally resilient.

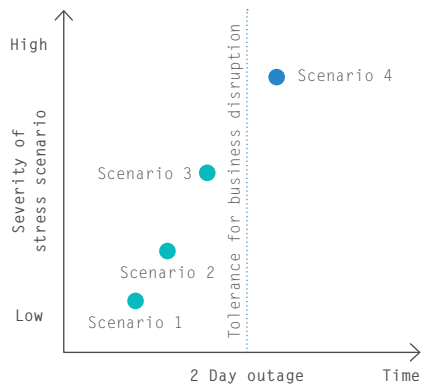
### ANNUAL REVIEW

While changes to processes should be made as soon as the need is identified (e.g. due to an event that has happened at a competitor) all the steps covered already should be reviewed on at least an annual basis to identify any changes and drive remediation. One key element is using scenario testing to prove that the firm can remain within its impact tolerances given disruption to its processes. This should all culminate in a new self-assessment document signed off by the relevant senior managers and the board.

EXAMPLES OF THE RESULTS OF SCENARIO TESTING

**CASE ONE:**

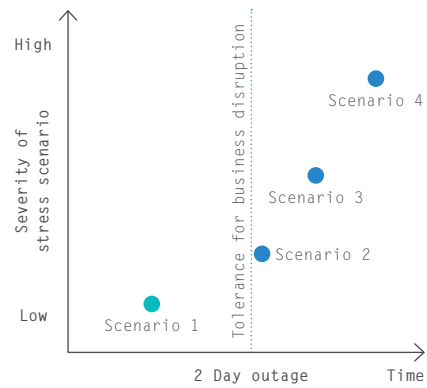
A firm considers its impact tolerance against severe but plausible scenarios. Here operational resilience is sufficient - it is disproportionate to expect the firm not to breach its impact tolerance in the extreme scenario of scenario 4.



● Scenario recovered within tolerance

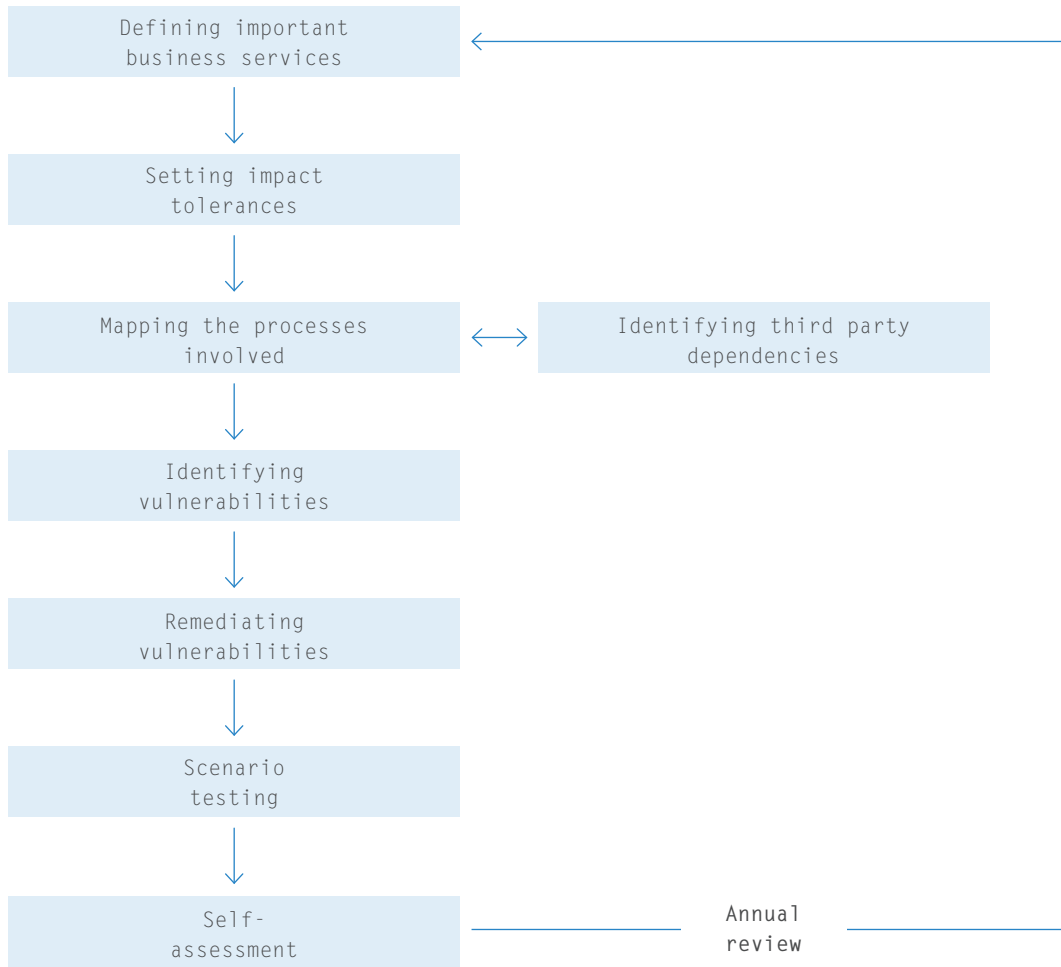
**CASE TWO:**

A firm considers its impact tolerance against severe but plausible scenarios. In this case, operational resilience is not sufficient - the firm should take steps to improve operation resilience.



● Scenario not recovered within tolerance

### THE STEPS INVOLVED IN OPERATIONAL RESILIENCE



## MANAGING THE RESPONSE

This quote is as true of responding to an event today as it was when written 2,500 years ago. Once an event is underway the training of the individuals involved in managing the response as well as the structures put in place beforehand will determine how successfully a firm responds to the challenge. There will not be time to extemporize a well-founded response.

Identifying the right decision-making body and the freedom and constraints of their decision-making is the starting point. Too small and it is not representative of all relevant stakeholders while too large and it becomes paralysed and unwieldy. Who is ultimately the responsible for decision making and what influence can other members of the forum exert? The factors that determine the answers to these are largely firm specific but all individuals will need to be trained.

Training should include the nature of some possible disruptions such as the types of cyber threat and as well as the end to end processes for the business to enable better discussion and challenge when the inevitable happens. More importantly, it should cover and rehearse decision-making in fast paced environments based on incomplete information. This is typically very different to normal decision-making due not only to the compressed timeframe but also to the much greater number of variables. (e.g. a trader may face having to make a choice in a similar timeframe but will typically face binary decisions – whether to go long or short).

Information is not only key but will also likely be more fragmented making the creation of a picture of the situation far harder. Information needs to be filtered and presented in a way that allows executives to make the best decisions possible and remain focused on the more critical items.

This MIS on process status should be designed in from system inception and allow for rapid aggregation. Information on the status of a firm's processes should be readily available and visualized in a way that facilitates understanding. Best Practice,

for example, would be where the CHAPS interface sends a confirmation to a central dashboard that the daily feed has been sent (and received at the other end). SMEs should also be available to support decision making.

Communications is a key element in managing the response, critically to customers but also internally, to regulators and potentially other market participants.

Firms should look to create a central control point through which information and decision making is channeled and tracked.

Practice makes perfect and all elements of the event response apparatus need to be rehearsed regularly in response to simulated events to be effective. After each rehearsal a thorough review should be held to identify any issues.

“

*Every battle is won before it is fought.*

”

Sun Tzu – The Art of War

Efforts should be made to learn from non-financial organizations such as the UK Armed Forces who are experienced in decision-making in fast moving situations to ensure that best practice is adopted. One approach used by western militaries is the concept of the OODA loop. This is a way of breaking down the response to fast moving situations into phases that then allows each one to be focused on and improved in terms of quality of decision making and timeliness so when recombined the loop is run at pace to gain and retain the initiative. This can be adapted to managing a response in an operational resilience context.



OODA LOOP CHECKLIST

OBSERVE, ORIENT, DECIDE, ACT: A MILITARY APPROACH TO COPING IN A CRISIS

**One highly effective tool used to help Western Militaries understand and improve their decision making in response to fast moving events is the concept of the OODA loop. Each of the four phases (observe, orient, decide and act) is taken in isolation, improved in terms of both accuracy and time taken, and then recombined and run repeatedly as a cycle at pace to gain and retain the initiative. In Business Continuity Planning (BCP) there are events rather than enemies but the same approach leads to better (and faster) decision making. Here we outline some of the factors and considerations that apply in a BCP situation under the phases of the OODA loop that can help frame your thinking, particularly at the current time.**

RECEIVE INFORMATION ON THE EVOLVING SITUATION

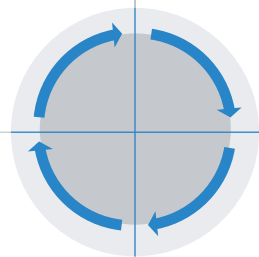
1. Are you in touch with regulators and local authorities?
2. Do you have an adequate flow of information about your business services and people across geographies?
3. Have you nominated someone to stay abreast of the latest information?
4. Is the effectiveness of the steps that you have taken so far being monitored?
5. Are there established communications with your third-party suppliers BCP functions?

OBSERVE

ORIENT

UNDERSTAND WHAT THE INFORMATION ACTUALLY MEANS

1. Do you understand their impacts over time?
2. Have you mapped critical functions and who is required to perform them?
3. Have you modelled the impact on your clients?
4. Are all factors around delivering services identified along with the sensitivity to them?
5. Is there a 'War Room' to keep track of your firm's status and act as a control point for all information?
6. Have you reviewed the information through the lens of legal entity?



IMPLEMENT DECISIONS

1. Are there designated individuals who will ensure that decisions are actioned?
2. Are there clear communications to your teams, clients and suppliers on current impact and actions you plan to take in the future?
3. Are the steps you are taking straightforward?
4. Are you physically reinforcing those steps by restricting access etc. where possible?
5. Are you operating through the normal management chain?

ACT

DECIDE

DEVISE, EVALUATE AND SELECT COURSES OF ACTION

1. Is the right governance structure in place?
2. Have clear priorities been agreed and set for short and medium term?
3. Has one individual been assigned overall responsibility?
4. Do impacted areas all have representation?
5. Are the board and regulators being updated on a regular basis?
6. Have you considered how you will unwind the actions that you are taking?
7. Is information being logged on a timeline to allow for lessons learned?
8. Have you considered setting up a red team?
9. Does the plan account for situations in which key individuals are not available?

## LEARNING THE LESSONS

Nothing stands still and neither can preparations to ensure a firm's resilience. Events that happen to other firms should be studied carefully to see if lessons apply and changes are required to avoid a similar event occurring.

This should involve not just other firms in financial services but right across the spectrum of relevant organizations (Did Travelex<sup>7</sup> absorb the lessons of the WannaCry ransomware attack on the NHS in May 2017<sup>8</sup>?).

The same goes for the outcome of events, real and simulated, that happen to a firm directly. There should be robust 'post-mortems' for service disruptions to ensure that all lessons are learned and that the resilience arrangements worked as intended. These should be documented to demonstrate reasonable steps taken in supervision.

At the very least, this review should be part of the completion of the annual self-certification process. The harder a firm prepares and trains to manage events the better the outcome when the inevitable happens.

“

*It's tough to make predictions,  
especially about the future.*

”

Yogi Berra

## WHAT NEXT?

The increasing complexity of the financial ecosystem and with it the greater risk of disruption warrants a greater focus on how to manage when the inevitable event happens. The key to firms successfully remaining within defined impact tolerances when there is a disruption is in the thoroughness of the preparations, realism in rehearsing the systems and the team involved in managing the response and the rigor with which lessons are applied. A self-critical approach where disruptions are expected, and an open culture focused more on addressing mistakes and issues than identifying who is to blame will improve a firm's likelihood of being operationally resilient.



## REFERENCES

- <sup>1</sup> <https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf>
- <sup>2</sup> <https://uk.reuters.com/article/uk-tsb-report/tsb-and-parent-sabadell-heavily-criticised-for-it-crash-that-locked-2-million-out-of-accounts-idUKKBN1XT176>
- <sup>3</sup> <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp2919.pdf>
- <sup>4</sup> <https://www.fca.org.uk/publications/consultation-papers/cp-19-32-building-operational-resilience-impact-tolerances-important-business-services>
- <sup>5</sup> [https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA\\_revised\\_Guidelines\\_on\\_outsourcing\\_arrangements.pdf](https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA_revised_Guidelines_on_outsourcing_arrangements.pdf)
- <sup>6</sup> <https://abcnews.go.com/Business/company-loses-190-million-cryptocurrency-ceo-dies-sole/story?id=60851760>
- <sup>7</sup> <https://www.bbc.co.uk/news/business-51034731>
- <sup>8</sup> <https://www.bbc.co.uk/news/health-39899646>

# GETTING READY: CHALLENGES TO MEETING THE UK OPERATIONAL RESILIENCE REGULATION

---

AUTHOR:  
Will Packard, UK

In the post COVID-19 world, firms across financial services with regulated UK legal entities are focused on how to address the proposed operational resilience FCA/PRA regulations, as set out within the consultation papers issued jointly by the Bank of England, Prudential Regulatory Authority (PRA) and Financial Conduct Authority (FCA) at the end of 2019.

They face several challenges due, in part at least, to the outcomes-based approach of the UK supervisory authorities which introduces a level of subjectivity into the compliance preparations. We will discuss some of the more significant challenges in this paper as well as outlining some ways to mitigate them.

“

*A key priority for the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) is to put in place a stronger regulatory framework to promote operational resilience of firms and financial market infrastructures*

”

Bank of England, December 2019

## IT'S NOT WHAT YOU DO, IT'S THE WAY THAT YOU DO IT

### DEMONSTRATING COMPLIANCE WITH THE REGULATION

The proposed regulation is different from much that has been implemented recently in that it is focused on a broad outcome and the approach that firms should take to achieve it, rather than specifying a clearly defined end-state. This is evident in the way the regulators do not expect firms to be able to maintain services in every eventuality; they expect firms to indicate in their self-assessments the scenarios they passed and the ones that they did not. Approaches are harder to evidence in terms of compliance requiring a clear record, at each stage, of the logic behind decisions taken.

“

*Firms need to tackle their operational resilience preparations with a real sense of urgency.*

”

## A HIGH BAR TO REACH

### DO NOT UNDERESTIMATE THE LEVEL OF PROOF THAT BOARDS WILL REQUIRE

Legal entity boards are required to sign off their firm's self-assessment confirming that it is operationally resilient. Board members, under the terms of the UK's Senior Manager & Certification Regime (SMCR) and the personal liability that entails, need to demonstrate that they have taken reasonable steps in carrying out their duties. In this case, that means ensuring that the chosen approach is sound.

Non-executive directors, who will only touch the topic in board discussions, will feel this particularly acutely given that any event causing significant disruption is likely to be dissected to a greater extent than, say, a failed business strategy. This raises the bar significantly in terms of the evidence required to demonstrate that the approach taken and the logic behind related decisions at all stages was sound.

It is likely that getting board approval will be an iterative exercise to accommodate refinements requested by board members. This will take time, and that should be factored into the project plan and not left to the last minute. The key message here is to engage boards early on.

## ONE SIZE DOES NOT FIT ALL

### EVERY FIRM WILL NEED TO DO THEIR OWN ANALYSIS

Firms need to identify the Important Business Services (IBSs) that they provide to clients within their wider offering and set impact tolerances. The regulators have explicitly given firms these freedoms and expect a clear logic to be applied when selecting these IBSs and in deriving impact tolerances. While on the surface the offerings of many firms may appear similar, there are critical differences in the details, such as customer types, specific product offerings and geographical coverage. Accordingly, every firm will need to approach this selection process to an extent with the proverbial ‘clean sheet’. Sufficient time should be factored into their plans to accommodate this.

“

*It is unlikely that firms will get everything right first time.*

”

## THE PROOF OF THE PUDDING

### SCENARIOS NEED TO BE SELECTED CAREFULLY TO MAKE THE TESTING VALID

Scenarios used in the testing phase should be severe but plausible and cover a range of events. The regulators do not specify precise scenarios for which firms should be prepared. It is likely, however, that COVID-19 would have been out of scope at the time the consultation papers were first published in December 2019, as few would have expected over a quarter of the world’s population to be locked down at home less than six months later.

Given the role that this testing plays in providing boards with the required level of comfort regarding their firm’s operational resilience, this is a key area to get right. The number of scenarios is not stated (though the example diagram in the PRA consultation paper indicates four). To be a ‘fair’ test, the scenarios should ideally be selected by parties other than the teams responsible for the operational resilience framework so that the results can be shown to have not been gamed.

## PULLING TOGETHER

### DELIVERY PROCESSES NEED TO OPERATE SEAMLESSLY ACROSS INTERNAL BOUNDARIES

To reflect the customer perspective looking vertically through the firm, responsibility for the delivery process for an IBSs may be split across business functions and reporting lines and across geographies. All stakeholders involved in a specific process, including any third-parties, will need to work together to ensure that an impact tolerance is not breached; this demands a degree of transparency and trust.

In rehearsing the scenario, clear roles and responsibilities should be defined and codified in preparation for any disruptive event. Where impact tolerances are tight, the risk is that merely standing up the individuals responsible for running the remediation process can take a significant amount of time, exacerbating an already tight situation.

## TONE FROM THE TOP

### SENIOR OWNERSHIP AND DRIVE IS NECESSARY TO ACHIEVE THE RIGHT FOCUS

Regulators are expecting management teams to take the lead in implementing the agreed approach. In the past, when firms have delegated the task to individuals too far down the organizational chain, it has proved a struggle to ensure the required level of focus and spend is committed to meet regulators' expectations. Firms should look to have a standing agenda point at meetings of their principal executive committee that covers operational resilience in order to ensure it receives the necessary level of buy-in and commitment from senior leadership.



## COVID COMPLACENCY

### THE NEXT EVENT WILL BE DIFFERENT

COVID-19 was unusual as a disruptive event.

Firms in the UK had approximately 6 weeks' forewarning that trouble was coming. Normally the first that a firm's leadership team will be aware of an event is after it has happened.

While staff were impacted by the virus, infrastructure was less dramatically affected. Provided remote working was possible for a sufficient number of staff (and this was hard for some), then firms were able to cope with the first order effects.

Firms were all impacted more or less at the same time in the UK, so the pressure to respond was shared across sectors rather than being concentrated on one firm.

The flip side of this was that many locations across the globe were impacted simultaneously, so BCP plans relying on just one disaster recovery location were not sufficient to cope with such widespread disruption.

At the start of 2020, it was almost inconceivable that individuals might be locked down for such extended periods of time. Hence plans that only envisioned short-term disruption have needed to be rapidly revised.

Fortunately for firms, points 1-3 (amount of notice, minimal infrastructure impact and COVID's universality) mitigated points 4 and 5 (the geographical and duration impact).

Next time a firm is unlikely to face a similar set of circumstances, so surviving COVID-19 does not ensure readiness for the next disruptive event. Plans should therefore be stress-tested to confirm that firms are well positioned to cope with a diverse range of scenarios. Train hard, fight easy is the order of the day.

## THE SMALL UK BRANCH SITUATION

### REASONS TO PUT THE OPERATIONAL RESILIENCE AT THE TOP OF THE AGENDA

The FCA regulates well over 1000 legal entities and these will all be covered by the new rules. While many legal entities will be the principal vehicles used by firms to transact business, some will be merely a small part of a larger operation headquartered outside the UK. In such cases, most of their services in the UK will be delivered via the same processes as other services globally. So compliance with UK regulation for what is in effect just a small proportion of their business may seem disproportionate in the eyes of such multinational firms.

This may strike some as a reasonable argument, but there are a couple of mitigating factors to consider. The UK supervisory authorities' approach to operational resilience, while rigorous, is well thought out and logical. If applied correctly, it will enhance a firm's resilience with clear lines of sight for management regarding those services that should be protected and the level of protection needed.

Given the cost of disruption, both direct and in terms of potential sanctions, compliance with the proposed regulations will have significant benefits – both at home and beyond. The impact of these UK regulations is undoubtedly being watched carefully by regulators globally and, if deemed effective, are likely to be copied in other markets, albeit with local variations. In short, for multinational firms there are benefits to implementing the UK's approach to operational resilience as a standard, since compliance with very similar rules is likely to be required across multiple markets and locations.

## TIMING IS EVERYTHING

### THE DEADLINE IS TIGHTER THAN IT APPEARS; FIRMS SHOULD DEVELOP A SENSE OF URGENCY NOW

While the December 2023 compliance deadline mentioned in the consultation papers is more than three years away, the UK supervisory authorities indicate that more complex and systemically important firms will be expected to have completed their preparations sooner than that date.

The FCA and PRA stated on 7 May 2020 that they do not expect firms to be ready before the end of 2021, with the clear inference that they expect the more complex firms to finish their preparations by early 2022. These firms should be addressing the task now with a sense of urgency if they are to meet this timeline.

## THE KNOWN UNKNOWNNS

### THE AMOUNT OF WORK REQUIRED WILL ONLY BE KNOWN HALF-WAY THROUGH

Until firms have identified their IBSs and set impact tolerances, it will not be possible to get a clear idea of the amount of work required to ensure their delivery processes are resilient. Adding to the pain, remediating vulnerabilities is likely to take the most time to complete of all the required steps. Given the proposed timeline for compliance, firms need to start making strides as soon as possible to set their programmes in motion, with the necessary resources and approach agreed, or risk significant delays.

## THE END OF THE BEGINNING

For many firms, there remains a great deal of ground to cover over the next few months. Firms need to tackle their operational resilience preparations with a real sense of urgency. The spirit of the proposed regulations encourages an approach to operational resilience that is ongoing and iterative in nature (as indicated by focus on lessons learned and an annual refresh in the consultation papers) to ensure firms are properly prepared.

It is unlikely that firms will get everything right first time. While there may be challenges and even setbacks to navigate in the coming months, what is most important is that boards and management teams adopt a serious and thoughtful stance towards operational resilience, exhibit a sense of urgency in tackling the necessary steps and commit the required resources to this undertaking, in line with the expectations of the UK regulatory authorities.

---



NEW WORKING  
PARADIGMS

---



# COVID-19: EMBRACING BETTER WAYS OF WORKING IN THE NEW NORMAL

---

AUTHOR:  
Alla Gancz, UK

**COVID-19 has required firms to rapidly embrace remote working. This presents a unique opportunity to embed new ways of working in preparation for the new normal.**

Despite the existence of robust frameworks, strong employee demand and proven benefits, at the beginning of 2020 new ways of working had yet to be widely adopted. However, since then, we have seen companies shift abruptly to remote working arrangements, in some cases literally overnight.

Initially this was typically viewed as a temporary measure to ensure that firms and their employees could continue to operate effectively in the short-term. There was a sense of ‘treading water’ until the eagerly awaited end of lockdown was announced and business as usual could resume. But as the weeks have passed and government measures have been extended, there has been a growing realization that this new way of working is likely to persist for the longer term.

As they look to the future, financial services institutions can expect to move through three distinct phases as they refine

remote working, plan how they will reintegrate employees, and begin to lay the foundations for a workforce of the future and a more holistic talent strategy.

The first **rapid response** phase is a business continuity-driven adoption of remote working, and at this stage is mostly complete. The priority for firms now is the second phase of **adapt and enhance** in order to optimize ways of working.

The focus should be on enhancing the effectiveness of remote work, maintaining employee wellbeing, upskilling teams on remote collaboration to ensure key milestones are still hit, and ensuring that tooling is in place to allow teams to do their jobs. These should not be ‘sticking plasters’ that will leave institutions with a COVID legacy to solve for but rather robust strategic enhancements.

Finally, the third phase is the transition into **the new normal** that will emerge post-COVID, and the potential pivots required as part of that journey. Central to that is a reimagination of what the workforce of the future looks like and an openness to embracing a new model of business as usual.

THE COVID-19 RESPONSE PHASES



**RAPID RESPONSE**  
Accelerated remote adoption-already completed

- Enable remote working for relevant employees ensuring employee wellbeing, data security and remote tooling is considered
- Implement rotation patterns for work that requires a physical presence
- Rapid shift in working culture
- Rapid resource redeployment
- Update working patterns and tailor guidance to staff based on their individual circumstances

**TACTICAL RESPONSE COMPLETE**

**ADAPT AND ENHANCE**  
Optimize ways of working

- Enable employees to operate effectively, collaborate and deliver successfully
- Ensure employee wellbeing during lockdown and in extended recovery mode
- Ensure business and operational resilience alongside risk mitigation measures
- Deploy resources strategically and ensure proper training
- Plan for the return and reintegration of the workforce
- Identify cost optimization opportunities

**HIGH PRIORITY FOCUS**

**BE READY FOR THE NEW NORMAL**  
Establishing future ways of working

- Plan for the post-pandemic economic downturn and recessionary environment
- Prepare for potential variance in new normal scenarios
- Plan your workforce of the future
- Leverage ways of working to differentiate your employee value and talent retention propositions
- Workforce reskilling and planning
- Plan for strategic program remediation
- Build resilience and agility into the business and supporting technologies
- Structurally assess and evolve cost base

**STRATEGIC FOCUS**

So why this pre-COVID resistance to the adoption of new ways of working? After all, prior to enforced remote working, employees almost universally saw it as an attractive benefit, with no less than 99 percent stating they would choose to work remotely, at least part time, for the rest of their careers [2019 State of remote work report Buffer.com]. Productivity concerns had been cited a key concern, but the data did not seem to back this up, with 85 percent of companies saying greater location flexibility led to an increase in productivity [Wundamail 2019 State of Remote work Survey].

Either way, the tone of the conversation has now changed – perhaps forever. Jes Staley of Barclays stated that “the notion of putting 7000 people in a building may be a thing of the past”. Forecasts from Global Workplace Analytics undertaken and published in April 2020 suggest that 25-30 percent of the workforce will be working from home for multiple days each week by the end of 2021.

“This is not how I envisioned the distributed work revolution taking hold,” Matt Mullenweg, chief executive of WordPress and Tumblr owner Automatic, noted. Mullenweg’s company is already ‘distributed’, and he predicts the changes could also offer “an opportunity for many companies to finally build a culture that allows long-overdue work flexibility”.

Employee choice is also expected to shape the new normal – indeed, it would be naïve to think this will be dictated by employers alone. Will employees want to go back to the way they worked prior to the crisis, having productively worked remotely for an extended period? Will staff challenge employers regarding the benefits of being present in the office? What might this mean from an HR, risk and cost base perspective?

There remain many unknowns and an even larger number of variables that will influence what happens next – and by extension, engagement with new ways of working. But there is also a certainty that things will not simply revert to pre-COVID conditions. Companies that can offer their workforce the right tools, culture and operating structure to help employees through this transition to the new normal will emerge more focused, resilient and better positioned to prosper in a new competitive landscape.



CLARITY AROUND POST-PANDEMIC BAU IS YET TO EMERGE - BUT WILL VARY ACROSS ORGANIZATIONS BASED ON THEIR CULTURE AND DIGITAL MATURITY.

	DEGREE OF CHANGE	LIMITED CHANGE	MODERATE CHANGE	EXTENSIVE CHANGE
IMPACT AREA	Employee choice	Majority of employees return to work in the same patterns as pre-COVID	Increase in requests for remote working, given it has proved its feasibility during the pandemic	Employees look to employers offering 'newer' ways of working and leave those organizations not offering such flexibility
	Employer response	Remote working allowed as necessary or on request	Remote working proactively offered to particular segments of the workforce	Remote working embraced and enabled across the workforce, and used extensively by staff
	Location of work	Office workers return to the office with the same frequency – no tangible impact to long term office / location strategy	Remote working / rotation patterns enabled for specific teams	Remote working fully enabled. Implications for longer term planning around physical footprint, fixed overheads and global travel expenses
	Organizational structure	Traditional pyramid structure kept in place to ensure successful project execution	Some business units adopting more progressive frameworks and structures, such as Agile	Streamlined agile structure fully implemented and focused on smaller project teams and their results
	Leadership framework	Traditional leadership frameworks and styles, large programmes command and control, and approval gates	Teams move to a more agile, accountable and empowered framework	Focus moves to team accountability and a fail fast approach, with only strategy remaining centrally coordinated
	Workforce construct	Full-time employees make up the majority of the workforce	Management and key divisions remain full time but increased use of freelance workers	Full-time employees becoming the minority as organizations make extensive use of freelancers on an 'as needs' basis
	Resulting scenarios	Ways of working revert predominately to where they were pre-COVID. We see limited long-term changes in behaviours, strategies or workforce planning (except for adherence to government guidelines around social distancing).	Both employees and employers implement remote working based on balance, productivity and cost savings. Remote working is widely implemented within those organizations that are culturally ready for it and/or for those workers most suited to it.	Employees view 'remote' as the default option. Employers look to implement it to realize long-term cost savings and to attract/retain talent. These organizations embrace agile to ensure productivity is maintained in a remote environment.

## WHAT SHOULD COMPANIES DO?

- Ensure your teams are **thriving rather than surviving** in the new environment – and if not, create the culture, instil the behaviours and implement the tooling they need. It's also essential to protect your teams' mental health and wellbeing.
- **Maintain productivity** across key programmes by rapidly deploying agile and ensuring high-risk or critical programmes are kept on track by leveraging ways of working practices.
- In parallel, **plan proactively** for the reintegration of those elements of the workforce whose return is business critical. Don't wait for government mandates to commence your scenario planning and evaluate your options.
- Finally, **grasp the opportunity to reimagine the art of the possible**. Organizations can emerge from the crisis with an enhanced employee value proposition in place alongside a fresh perspective on cost reduction opportunities.

As we emerge from the initial and any subsequent lockdowns, firms will need to strike the optimal balance between adhering to government guidelines, respecting the desires of their workforce and delivering on their own goals. Those financial institutions that grasp the opportunity to reassess, reengineer and reimagine their workplace in a proactive fashion will be best placed to offer a differentiated employee value proposition, and will also reap the benefits of increased efficiencies and ultimately a significantly lower cost base.



## REFERENCES

Jes Staley quoted in the Financial Times – Office model hangs in the balance after Covid – May 3, 2020

Matt Mullenweg quoted in The Guardian – March 13, 2020:

<https://www.theguardian.com/technology/2020/mar/13/covid-19-could-cause-permanent-shift-towards-home-working>

Future workplace statistics:

<https://globalworkplaceanalytics.com/>

State of remote work:

<https://buffer.com/state-of-remote-work-2019>

# HOW TO REFRESH YOUR DIGITAL STRATEGY TO PREPARE FOR THE NEW NORMAL

---

AUTHORS:  
Alla Gancz, UK  
Cassim Virani, UK

Who could have predicted that the center of conversation for 2020 would revolve around coronavirus? At the time of writing, the world continues to battle the ongoing pandemic, which has impacted almost all countries, economies and populations in some shape or form. Changes to how we shop, how we work and even how we bank are now challenging the concept of what should constitute a normal service.

While the full impact of COVID-19 will not be known for quite some time, one trend has become particularly clear across most sectors – digitalization. In this article, we explore how customer banking expectations are changing due to COVID-19, banks’ reactions to the pandemic, and why a strong, digital strategy is so critical for banks to embrace and thrive in the ‘new normal’.

“

*We are entering a time when a strong digital strategy is becoming a necessity rather than a luxury – welcome to the new normal.*

”

## CHANGES IN CUSTOMER BEHAVIORS AND ATTITUDES

Well before COVID-19, online shopping and home delivery had become a normal part of everyday life for many people around the world. However, the current climate has seen a massive surge in the use of delivery and subscription services such as Amazon, Tesco, Ocado and Waitrose groceries, and Netflix, with the latter acquiring 16 million new global accounts in lockdown.<sup>1</sup> In addition to these types of services, digital-only banks are being looked upon as a blueprint for how to best operate as a financial services firm during uncertain times. Starling Bank, for example have used the pandemic to further simplify SME banking by adding three new integrations to its Marketplace: Slack the workplace messaging platform, Bionic, the energy switching service, and Equipsme, a health insurance provider.<sup>2</sup>

Our analysis has found that consumers are anxious about how to manage and plan their finances and how to cope with the new normal. With many brick and mortar banks temporarily closed, the dependency on online and mobile banking has skyrocketed. Six million<sup>3</sup> (12 percent) of UK adults reportedly made the switch to digital banking in the early weeks of the pandemic, simply by downloading their bank's digital application. With reduced in-person support, the analysis also found that a quarter of existing digital customers are using their banking apps more often during the crisis. We are confident this trend will continue and grow post-coronavirus.

However, the shift towards digital banking has raised valid concerns that the elderly and vulnerable, who make up millions of users, might get 'left behind'. While record numbers of customers aged 65 and above have reportedly moved to online banking since the crisis, not everyone in society will be able to make the switch.<sup>4</sup> Moreover, vulnerable people who embrace online banking could be especially susceptible to fraud, which was also risen during this period.<sup>5</sup> Whichever trends continue to emerge, it is clear that banks and other financial services providers must keep the diverse needs of these sizeable customer segments at the heart of their future strategy. Over a quarter of the UK's population consider themselves as vulnerable (26 percent)<sup>6</sup>, and the UK's 85+ age group is the fastest growing UK demographic and is set to double to 3.2 million by mid-2041.<sup>7</sup>

## HOW BANKS ARE RESPONDING

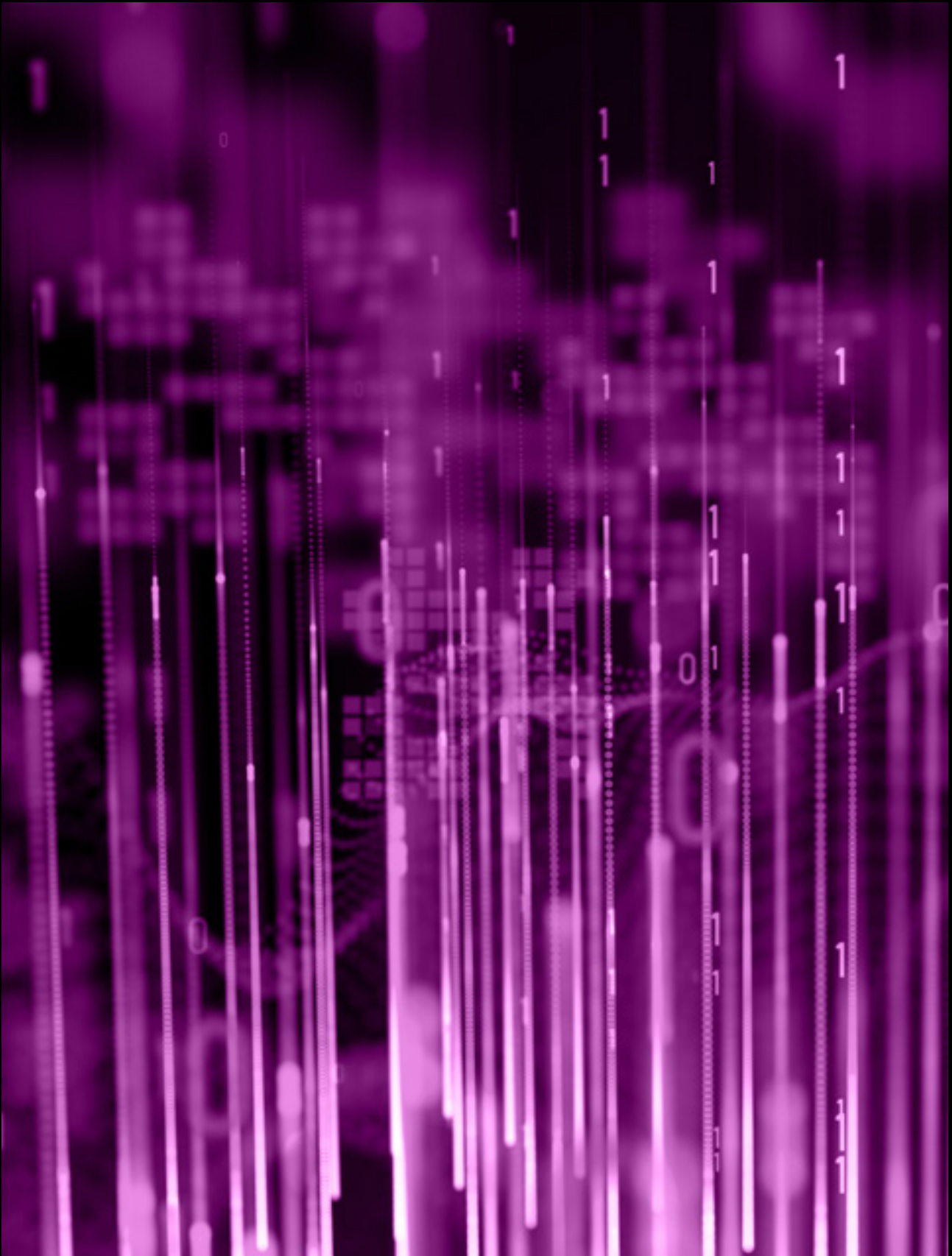
The COVID-19 lockdown has impacted those within the banking industry in several different ways, presenting both challenges and opportunities.

In order to curb the spread of the virus and adhere to strict social distancing measures, many high-street banks have reduced their services, such as Lloyds Bank and Barclays, who have closed a host of their locations. Customers are being urged to use telephone and online banking services rather than visit brick and mortar locations for safety reasons. Banks are now seeing call centers becoming overwhelmed with calls for support from customers – during the pandemic NatWest has seen a 730 percent<sup>8</sup> increase in the number of calls it is receiving.

Many businesses are fighting for survival and depend on vital lending support such as the Coronavirus Business Interruption Loan Scheme (CBILS). More than 300,000 firms<sup>9</sup> have made informal inquiries about seeking help from the scheme, and those looking to access support are finding it hard – with only 2 percent<sup>3</sup> successfully accessing the CIBIL program. A huge number of businesses (38 percent)<sup>10</sup> are even abandoning banking applications during the crisis due to slow due diligence processes.

As a result, banks are struggling to address key issues in supporting their customers getting access to the support they require, whilst also fending off threats from new entrants into the market, keeping an eye on their bottom line and setting up robust support models for the future. Even after COVID-19, more customers are expecting to do all their banking without having to leave the comfort of their sofa. So, what can banks do to prepare for the new normal?





## THE NEED TO BE PROACTIVE AND RETHINKING YOUR DIGITAL STRATEGY

Banks have a responsibility and an immediate need to manage and protect their revenue, processes, systems and employees during these uncertain times. However, these uncertain times also present banks with an opportunity to pivot and position themselves for the future through a thoughtful digital strategy and roadmap. With COVID-19's far-reaching impacts, digital strategies now require a **360-degree view** for banks, ranging from service models to talent and location strategies.

At Capco, we have observed that the coronavirus pandemic has further accelerated the move toward digital banking. **It is now crucial laggards follow suit.** We have identified three distinct phases that our clients can follow in order to address the key issues being faced now and support them in a productive manner on their journey to the new normal.

### PHASE ONE

The first phase is a **tactical response**, where banks take immediate actions to support their employees and customers in an operational shift. This phase will see banks will enable their workforce to operate remotely and see a rapid move toward digital channels. During this period banks will see a surge of calls into their call centers and will need to ensure that these calls can be answered, with vulnerable clients are prioritized. Working on having a flexible work force will help keep jobs, provide better customer service, and encourage their clients to continue banking and being active.

### PHASE TWO

The second phase focuses on the end-user, high-priority focus items. For instance, banks will need to review their customer journeys and ensure they are enabled to support digital channels, and how they can best support their customers, such as virtual help desks. Having more online and simple tools will make life much easier for their clients and reduce stress on call centers. During the phase, strategic and customized thinking will be need create a migration plan for how their workforce return to their in-person roles in a way that fits their culture and ways of working.

### PHASE THREE

The third and final phase is adopting a strategic focus, where banks will need to evolve their service model and get ready for the new normal. Banks must develop scenarios taking into consideration post pandemic factors, such economic client and the new normal way of operating. These scenarios will support the ability for our clients to re-invent their business models, imbed resilience and adapt and evolve their cost base and operational models. Generating prioritized initiatives to boost future growth based on market analysis and competitive benchmarking will ensure stakeholders are aligned on their future vision.

Based on the trends we have analyzed through customer interviews and current acceleration of digitalization, **having a dynamic and robust digital strategy is now more important than ever.** Financial services firms will need to be able to keep up with the evolving customer expectations and demands and be able to mitigate operational challenges in a proactive and agile manner. We are entering a time when a strong digital strategy is becoming a necessity rather than a luxury – welcome to the new normal.

## REFERENCES

- <sup>1</sup> <https://www.bbc.co.uk/news/business-52376022>
- <sup>2</sup> <https://www.starlingbank.com/news/three-new-integrations-in-business-marketplace/>
- <sup>3</sup> <https://www.moneyexpert.com/news/millions-downloading-banking-app-first-time-lockdown/>
- <sup>4</sup> <https://www.telegraph.co.uk/news/2020/05/11/over-65s-shopping-online-twice-much-lockdown-forces-get-tech/>
- <sup>5</sup> <https://www.which.co.uk/news/2020/05/the-hidden-cost-of-coronavirus-vital-fraud-protection-on-hold/>
- <sup>6</sup> <https://www.insurancebusinessmag.com/uk/news/breaking-news/aviva-on-how-the-insurer-is-battling-fraud-during-the-coronavirus-225215.aspx>
- <sup>7</sup> [https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/later\\_life\\_uk\\_factsheet.pdf](https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/later_life_uk_factsheet.pdf)
- <sup>8</sup> <https://www.bbc.co.uk/news/52208032>
- <sup>9</sup> <https://www.theguardian.com/business/2020/apr/15/covid-19-bailout-loans-issued-uk-firms-banks>
- <sup>10</sup> 38% of customers are abandoning banking applications for CBILs and Bounce Back loans – internally sourced from Capco client insight

---



TECHNOLOGY COST  
MANAGEMENT &  
OPTIMIZATION

---

# ACHIEVING MORE WITH LESS: TECHNOLOGY SPEND PRIORITIES OF A POST-PANDEMIC CIO

---

AUTHORS:

Olivier De Decker, France  
Julien Kokocinski, France

**CIOs have played a critical role in managing the COVID crisis to ensure continuity of business activities. Post-pandemic, they will need to invest smarter and more cheaply and to respond to changes – positive or negative – swiftly and efficiency. In this blog, Olivier De Decker and Julien Kokocinski, Partners at Capco, explore why a more structured and flexible approach to IT spend management is now more important than ever.**

Today, CIOs at many traditional banks are confronted with a complex situation. On the one hand, the pandemic is placing pressure on banks to rapidly cut costs. On the other, CIOs are expected to deliver important digital transformations and mandatory initiatives as banks adapt to the current conditions, including cybersecurity reinforcements or establishing the right infrastructure to allow people to work and collaborate remotely.

At the same time, as the uncertainty surrounding COVID-19 and its consequences continues, CIOs need to be in a position to adjust the levels of IT spend in response to evolving situations. This may mean reducing expenses in the event of a prolonged crisis or a slower-than-expected economic recovery; or alternatively, increasing spend to allow the organization, its infrastructure and project portfolio to be mobilized quickly to benefit from any recovery.

“

*A more structured and flexible approach to IT spend management is now more important than ever.*

”

## A COMPREHENSIVE AND TRANSPARENT VIEW OF COSTS VERSUS VALUE

To enable faster and more dynamic IT spend, the CIO must rely on a set of tools and data that creates an accurate and transparent view of the firm's IT landscape and project portfolio, including the cost, value and complexity of each element. Today, most banks do not have that view.

In fact, it would be fair to say that within many established financial institutions, the business and IT teams do not sufficiently understand each other. While IT managers are concerned with the cost of their network and servers, business line owners are not focused on these specific elements, but rather want to understand the headline cost of technology as it relates to their products and customers.

The CIO accordingly needs to articulate the IT budget in a way that speaks to the business in a transparent fashion. This would allow the CIO to provide clear guidance to the business on questions relating to the cost of launching a new functionality or increasing the scope of a product, or what cost reduction will result from a certain action.

“

*To enable faster and more dynamic IT spend, the CIO must rely on a set of tools and data that creates an accurate and transparent view of the firm's IT landscape and project portfolio, including the cost, value and complexity of each element. Today, most banks do not have that view.*

”

## ROI ON THE LINE

Cost-cutting is another example of where the CIO – and the business – need to have full transparency and understanding regarding immediate gains versus intrinsic value and longer-term impact. When banks need to cut costs, it is the ‘change bucket’ that usually suffers first, being deemed the softest target. Typically, change projects that heavily impact IT will be stopped, postponed or slowed down to reduce expenditure, and this also impacts the balance between the bank’s internal and external workforce. These adjustments need to be made in an intelligent fashion that avoids reducing resilience and hence putting the bank at risk. If CIOs do not have a clear view of return on investment (ROI) across their IT expenditure, this becomes difficult to achieve.

“

*The CIO needs an effective solution to analyze the ROI of each investment or project and clearly assess value and impact.*

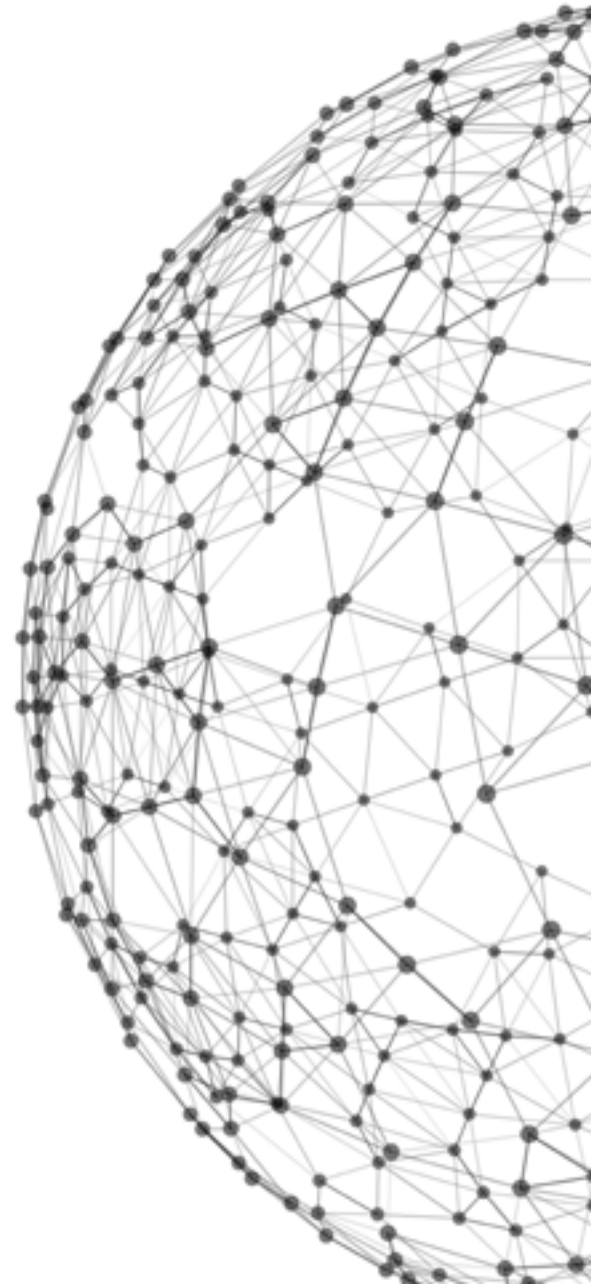
”

However, postponing or slowing down transformational initiatives means that important process improvements or customer experience innovations will not be achieved as planned, which may result in a loss of revenue in the future. Again, the CIO needs an effective solution to analyze the ROI of each investment or project and clearly assess value and impact. The CIO can then make data-backed recommendations whether to reduce or stop projects that are not vital or sufficiently revenue positive or, conversely, to increase investment in projects that will deliver a sufficient ROI.

## DATA IS KEY

An effective solution should be built around a multi-dimensional analysis of data for each IT application and project as well as business lines and products (considering elements such as scope, costs, income generated and resource consumption). That analysis can then inform decisions such as whether to discontinue a poorly performing product or business line or, alternatively, to transform it through additional investment.

Overall, this focus on data will enable the CIO to strengthen IT management and address the dual challenge of optimizing and prioritizing IT spend.



HERE'S HOW CIOS CAN IMPLEMENT A MORE FLEXIBLE APPROACH TO TECHNOLOGY SPEND MANAGEMENT AND DEMONSTRATE THE VALUE OF THE IT FUNCTION.



1. ENSURE TECHNOLOGY COST TRANSPARENCY

Technology cost transparency (TCT) provides visibility into cost drivers, technology resource consumption and cost information in respect of the balance between business and IT functions. This ensures that any adjustments reflect the most appropriate level of expenditure and offers the ability to forecast demand for technology services and to simulate the impact of change.

TCT seeks to establish a mentality that orients technology by service, with defined service levels and clear pricing. It translates IT services, process expenses and resource consumption into business functions and generates understandable metrics to enable key strategic decisions, as well as providing solid governance and a continuous improvement framework.



2. MEASURE PERFORMANCE AND BUSINESS VALUE OF THE IT FUNCTION

The CIO needs to move from being a cost center to become a strategic partner within the bank. Strong CIO performance requires IT to be managed as a business, through the application of best practice and benchmarking against the market to clearly demonstrate the value of the IT function.



3. CREATE THE RIGHT CONDITIONS FOR OPTIMIZING COSTS EFFICIENTLY AND SUSTAINABLY

This involves identifying cost reduction opportunities and assessing their potential and feasibility in the context of both BAU and projects, as well as prioritizing projects that offer a quick ROI and establishing a continuous optimization culture among IT managers.



4. INCREASE ELASTICITY OF TECHNOLOGY COSTS

CIOs can help direct their banks to make better choices through technologies and contractual models that enable a transition from fixed to variable costs, such as cloud or as-a-service solutions. Reducing the ratio of fixed costs helps adjusting the cost base quickly in case of downturns.



5. INCREASE ELASTICITY OF HUMAN COSTS

Firms need to deploy the right IT skills, at the right time and in the right quantity, to meet market and customer demands. This requires building a flexible technology talent ecosystem and tapping into larger skill pools through partner networks, remote working arrangements, upskilling existing workforce, as well as continuously reviewing strategic sourcing and partnership strategies to reflect the skills and IT capabilities required to meet business needs.



6. ADOPT AGILE APPROACHES FOR MANAGING BUDGET AND PROJECT PORTFOLIO

Agile portfolio operations and Lean governance can maximize value for the business by enhancing operational excellence, ensuring compliance and increasing adaptability to change.



## CONCLUSION

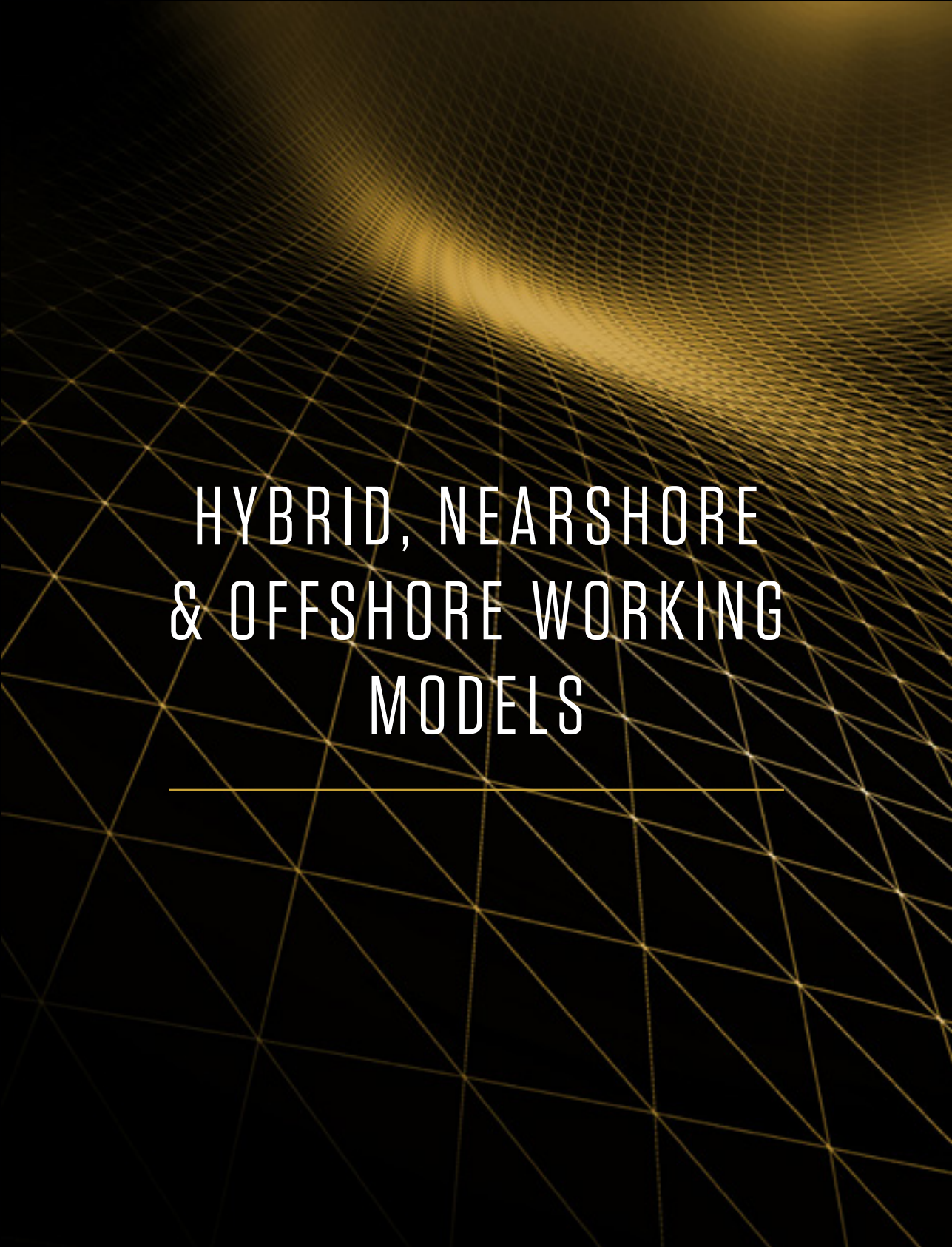
The need for transformation has been a constant theme for banks since the financial crisis of 2008, and the pressures arising from continuous regulatory change, increased competition and rapid technology evolution are nothing new. However, the 2020 global pandemic has radically increased these pressures and banks have no choice but to adapt to new working models and changing customer expectations.

CIOs have played an important role through the pandemic, ensuring continuity of services. Now, as they are facing significant cost constraints while at the same time looking to accelerate strategic technology projects, CIOs need to evolve from being a cost center to becoming a valuable business partner to help banks transform their activities and the way they serve their customers.

CIOs must position themselves at the center of the dialogue between the business and IT to ensure that they speak the same language about IT costs and partner effectively to make smart investments, maximize benefits to the bank and increase ROI.



---



HYBRID, NEARSHORE  
& OFFSHORE WORKING  
MODELS

---

# HYBRID, NEARSHORE AND OFFSHORE: CHOOSING THE CORRECT POST-COVID WORKING MODEL

---

AUTHORS:

Stefan Egg, Austria  
Peter Gallo, Slovakia  
Jana Porubská, Slovakia  
Branislav Kuzela, Slovakia  
Viera Novotná, Slovakia

Since it was first identified in late 2019, COVID-19 has claimed millions of lives and has caused significant operational and commercial disruption for companies worldwide. However, financial services were better positioned than most industries to weather the initial storm. Digitalization initiatives were in many cases already underway, and institutions were accordingly able to pivot quickly to accommodate remote working arrangements for most of their employees, ensuring a relatively high degree of business continuity.

The financial services industry is now focused on the journey towards a post-COVID new normal. Financial institutions that grasp the opportunity to reassess, reengineer and reimagine working models in a proactive fashion will be best placed to reap the benefits of increased efficiencies, productivity and ultimately a significantly lower cost base. In this paper, we detail the four working models available to firms and examine the pros and cons of each.

“

*Those financial institutions that grasp the opportunity to reassess, reengineer and reimagine their workplace in a proactive fashion will be best placed to offer a differentiated employee value proposition, and will also reap the benefits of increased efficiencies and ultimately a significantly lower cost base.*

”

## WORKING MODELS, PRODUCTIVITY AND COST SAVINGS

There is a clear recognition that alternate working models have both proved effective from a productivity perspective and offer the potential for cost savings. Current remote working environments and collaboration models have been defined rapidly to address the challenges posed by the pandemic. This has reopened the debate over what constitutes the optimal shoring model.

In the current environment, near-shoring elements of your operations certainly appears compelling – but which processes or functions should you choose? In reality, a hybrid operating, multi-sourcing model combining the different options set out below will in almost all cases prove the most effective approach. At the same time, finding the right balance between them is a challenge, being dependent on individual operating models, technology infrastructures, the status of digitalization programmes, and organizational flexibility.

## FOUR DIFFERENT WORKING MODELS

Today's COVID working environments and collaboration models were by necessity rapidly defined and implemented, and that abrupt change has served to recalibrate perceptions about future working paradigms.

There are four different options to consider: onsite, remote, nearshore and offshore. Every location model has its pros and cons:

- **Onsite** remains the preferred environment when dealing with sensitive and confidential information and for optimizing collaboration. Regulations also require that some functions or activities be based onsite in the local jurisdiction. However, it is often also the most cost intensive option.
- **Remote** or home working can offer a quieter environment than an open plan office space, and has additional benefits for employees in respect of travel and childcare, while for employers it can reduce real estate-related costs (if they choose to reduce office space). However, it is generally felt to have a negative impact on collaboration and teamwork due to a lack of in-person interaction.
- **Nearshore** can generate cost savings while maintaining similar cultures and time-zones, but there may be differences around ways of working.
- **Offshore** maximizes cost savings but minimizes available collaboration time and will require greater recognition and accommodation of cultural and language differences.

## ONSITE

Working onsite has long been the standard for most companies. The advent of the internet and advances in telecommunications have seen a gradual but over time tangible change to office working practices. Today<sup>1</sup>, over 50 percent of people would prefer to work remotely. In fact, an IBM study of 25,000 adults in the US in the month of April 2020 found that 54 percent would like to primarily work from home once offices reopen.<sup>2</sup>

In contrast, Global Workplace Analytics, in its Global Work-from-Home Experience Survey (first half of 2020), shows that only 16 percent globally want to leave the office permanently, with most preferring a mixture of both. Spending about half the time at each location seems to be the sweet spot for both the US and Europe.<sup>3</sup>

Let us take the opportunity to review all the advantages and disadvantages of onsite.

### BENEFITS

- **Teamwork and collaboration**

As the author John C. Maxwell famously noted: “Teamwork makes the dream work.”<sup>4</sup> When working onsite, a strong bond and connection between colleagues and teams typically develops, lines of communication and feedback loops are cleaner, and it is the optimal environment to foster collaboration to achieve common goals and complete tasks.

- **Motivation and productivity**

When working onsite, employees are on hand to boost one another’s morale. Teammates can literally step in to help each other if a colleague is stuck on a solution to a certain problem. Their physical presence allows for much more instantaneous communication and feedback than through virtual means.

- **Direct control**

If there is a problem, onsite allows for direct control via ‘hands on’ involvement of key personnel, and fast access to other experts outside the team.

- **Confidentiality**

When dealing with client data, it is usually required to work on secure premises and within certain hours to ensure client confidentiality.

- **No digital disruption**

Onsite allows for easier monitoring and management of employees’ activities.

- **Centralized infrastructure and support system**

Being onsite offers a more efficient work setup, for instance a fast and stable internet connection, powerful workstation, additional monitors, and access to printers. If you have a problem with hardware or software, IT support can typically be contacted in person rather than just addressing the issue over a dedicated helpline.

- **Culture**

In-person interactions can foster and improve relationships<sup>5</sup>, which in turn serves to reinforce a positive and inclusive company culture.

### CHALLENGES

- **High utility costs**

Maintaining a furnished, equipped and staffed physical space to house your employees is not cheap; an office location is a significant fixed cost that generates further costs that ultimately negatively impact a company’s bottom line.

- **Commuting**

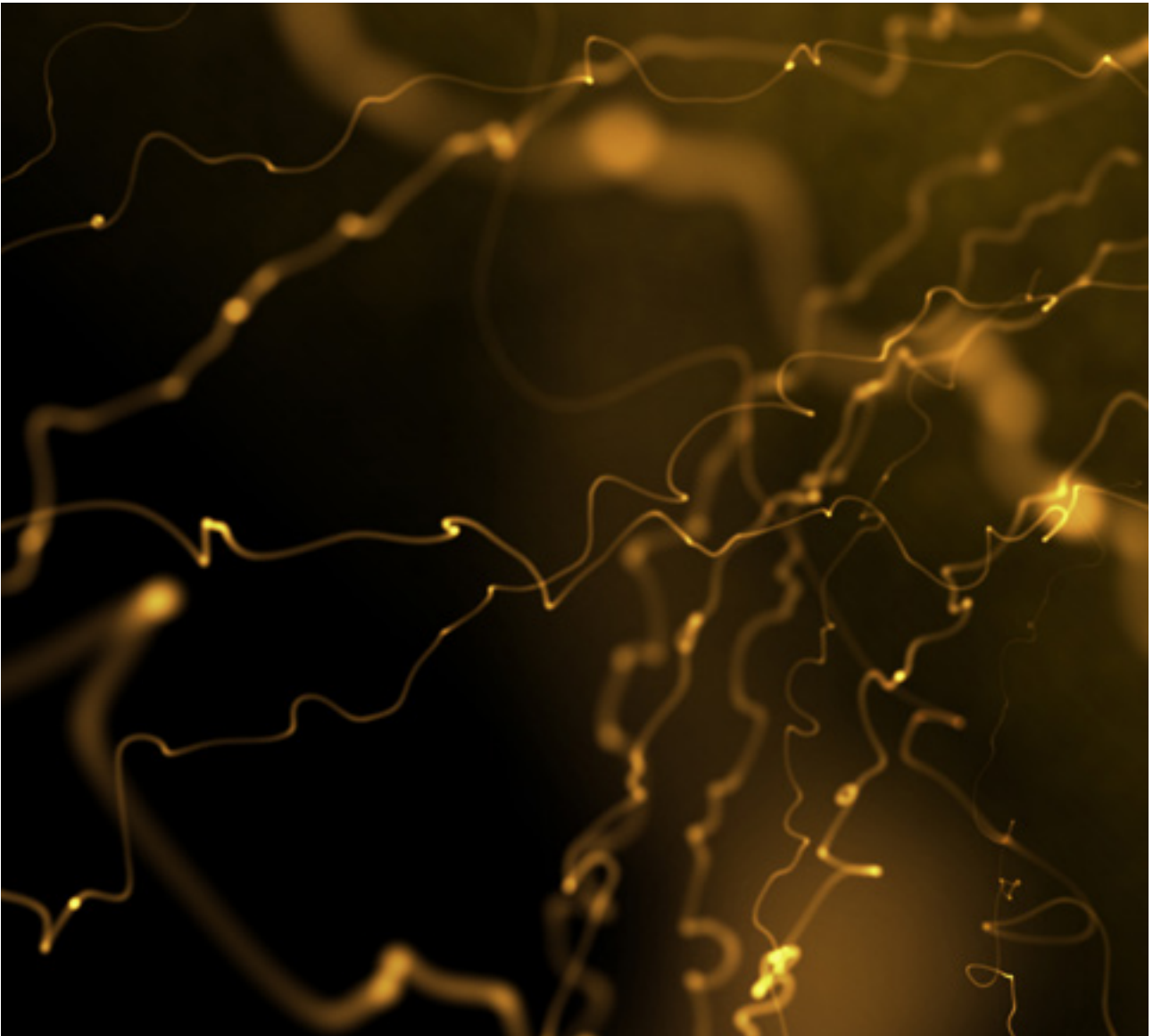
In contrast to onsite working, home working saves a significant amount of travel time and reduces associated costs, especially for those employees with long commutes. Commuting is particularly associated with significant psychological and social costs, which is why many would agree that eliminating the daily commute is beneficial in reducing stress levels.<sup>6</sup>

- **Distractions**

An office, especially one with an open plan layout, can prove a distracting work environment, with plenty to disturb an employee’s concentration and detract from their performance.

- **Health**

There is an increased risk of contracting infectious diseases when travelling by public transport<sup>7</sup> or having direct contact with others in an office setting.<sup>8</sup>



Of course, in some cases working onsite is obligatory, whether for regulatory reasons (e.g. trading desks), compliance purposes, or due to the handling of sensitive client data. Many banks or financial institutions do not trust VPNs or similar solutions, preferring that employees remain in a building where key operational factors can be more closely controlled. It is also worth noting that there are still elements of the financial services business that rely on paper (e.g. letters of credit). For those processes yet to be touched by digitalization, there remains a clear need for onsite working.

#### WHAT NEXT?

In future, we believe there will be even less justification for onsite work as issues such as ensuring computer network security will be given more of a priority, and clients will in turn trust solutions more. If one good thing has emerged from the ongoing pandemic, it is the shifts in attitudes toward remote working by a growing number of firms today. Has it ever had such a strong use case as now?

## REMOTE WORKING

Remote working – whether or not it has been at the top of the agenda for some organizations to reduce their footprint, lower their overhead and ultimately increase profitability – has become a necessity for most organizations to protect the health and well-being of their employees and to prevent the further spread of COVID-19.

As a result of the ongoing pandemic, many financial services institutions have been forced to kickstart or reinvigorate their digital transformation plans, whether to adapt their processes to accommodate digital solutions to facilitate transactions, or to maintain communication between clients, suppliers and their own employees.

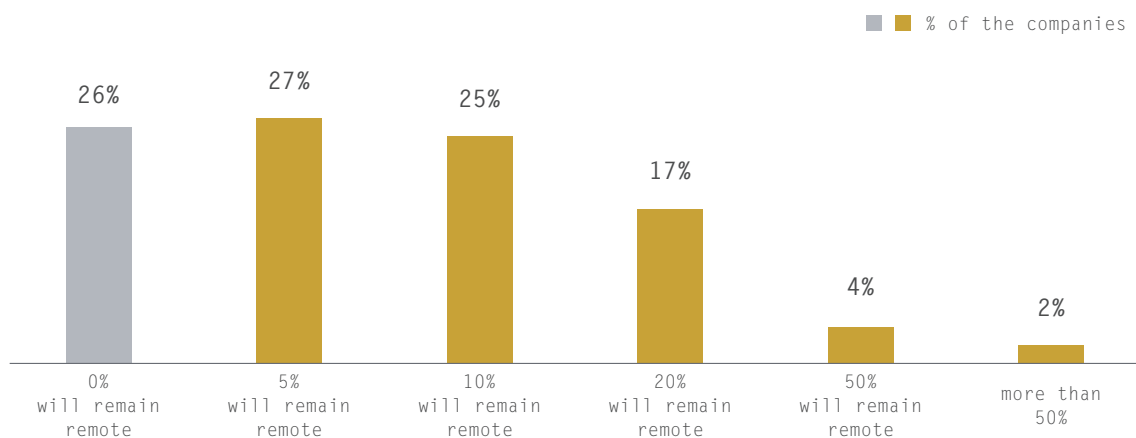
After years of talking about digital transformation but not truly acting upon it, the pandemic has demonstrated that many institutions were better prepared to embrace it than previously thought. Millions of workers have been able to deliver financial services remotely. The message is clear: remote work is no longer a luxury or privilege for employees – it is here to stay.

Remote work is about more than the right equipment and access to a private network, and it is also more than digital space and technology. It is about behaviours around communication and collaboration. Trust, accountability and individual outputs all need to be factored into this new normal working environment, as does identifying ways for workers to remain ‘human’ in this increasingly depersonalized (in the sense of fewer physical in-person interactions) working environment.

In the new normal, remote work could be a more permanent fixture than many realize: 74 percent of CFOs intend that at least 5 percent of their formerly onsite workforce will shift to remote working permanently post COVID, according to a Gartner survey<sup>9</sup>. Gartner also noted that almost a quarter of respondents said they will move at least 20 percent of their onsite employees to remote working permanently. Dingel and Neiman (2020) show that 37 percent of US jobs can be done from home, although this percentage varies significantly between cities and industries. Most jobs in finance, corporate management and professional and scientific services could be done at home.<sup>10</sup>

### 74% OF COMPANIES PLAN TO PERMANENTLY SHIFT TO MORE REMOTE WORK POST COVID-19

What percentage of your workforce will remain permanently remote post-COVID who were not remote before COVID?



Source: Gartner<sup>11</sup>

As many firms rethink their business models to make more extensive remote working a reality, they should not only consider the right technology, but also how to engender trust and implement new channels for regular communication, interaction and conducting other work-related activities. To this end, institutions can draw upon the experiences and practices that emerged during the initial period of the crisis.

## CHALLENGES

The transition from daily onsite office work to remote working can pose a range of challenges for employees and their managers.

- **Presenteeism and face-to-face management should become less important, as remote working shifts the focus from hours spent in the office to the delivery of specific objectives.** This requires outcome-based management of employees alongside new rules for communication, collaboration and feedback.
- **Creating a responsive technology to manage remote work.** It is not purely about having adequate equipment and infrastructure to access required applications and information, but also the infrastructure in the new home working environment, ranging from high-speed internet access to setting up multiple monitors, webcam and headsets.
- **Infrastructure needs to be secure.** Working remotely increases cybersecurity risks, so appropriate protection measures are crucial. The simplest solution is to use a VPN to secure both data and online connections. For financial institutions, it is particularly important to stipulate two-or multifactor authentication to secure client data, and also to monitor its use to ensure compliance.
- **Remote working devices should be managed by institutions.** A client's financial data is the most valuable and sensitive asset to a firm. Applications for monitoring remote workers activities can now check if the client's information is being manually copied to a computer or printed.
- **Remote working expenses and tax must be considered.** Additional remote working expenses, such as gas and electricity charges, internet access, and furniture costs need to be taken into account. Any impact on income tax should also be considered. Extra payroll tax registration should be in place in the event of remote working from a

different country when meeting thresholds relating to income generated or time spent.

- **Regulatory compliance must be adhered to.** The financial industry is a highly regulated sector with very strict requirements around the security of data and technology networks. Organizations will need to ensure that their employees remain compliant with the rules in a remote working environment.
- **Establishing work-life boundaries will encourage more engaged employees.** Employees can easily become overworked due to an inability to unplug from work, and there is evidence to suggest this is already happening due to the pandemic.<sup>12</sup> These boundaries should be agreed based on an individual's obligations and priorities.
- **Organizations must weigh-up how much remote work is manageable.** Not every office activity or process can be conducted remotely, and a realistic working model that combines home and office arrangement should be clarified and agreed.

## BENEFITS

Moving from daily onsite office work to remote working can yield a number of benefits for employees and their managers.

- **Lower utility costs**  
Remote working opens up considerable cost-saving potential for financial institutions, as it enables them to save a significant proportion of their fixed costs related to the rental of office space and equipment, as well as other operating costs calculated per employee that may have a negative impact on a company's overall profitability.
- **Less time spent commuting**  
Working from home saves the time spent commuting and reduces the associated costs, particularly for employees with long commutes. Many would also assume that avoiding daily commuting is beneficial in reducing stress and increasing job satisfaction and thus the well-being of their employees.
- **Elevated concentration and productivity**  
If employees work from home and were previously used to working in an open-plan office where their concentration was disturbed and their performance impaired, they are likely to



experience increased productivity.<sup>13</sup> In addition, they may spend less time in unproductive meetings and concentrate much more on completing their actual tasks and projects.

- **Health protection**

As the crisis has impressively shown us, social distancing and thus remote working reduces the risk of contracting infectious diseases when travelling by public transport or having direct contact with other people in an office environment.

- **Talent acquisition**

Remote working gives institutions access to a wider pool of applicants by enabling them to recruit qualified new talent irrespective of their actual geographical location and possibly in places where it has not previously been possible to seek or attract such talent.

- **Work-life balance**

Working from home can help employees and managers to better balance family life with their work commitments, as they are much more flexible in time and space when it comes to carrying out their work. For parents, this can lead to a more favourable work-life balance than if they only work onsite.

- **Employee retention**

Remote working gives employers the opportunity to develop new forms of collaboration and adopt a degree of flexibility that can increase the loyalty and stability of their workforce.

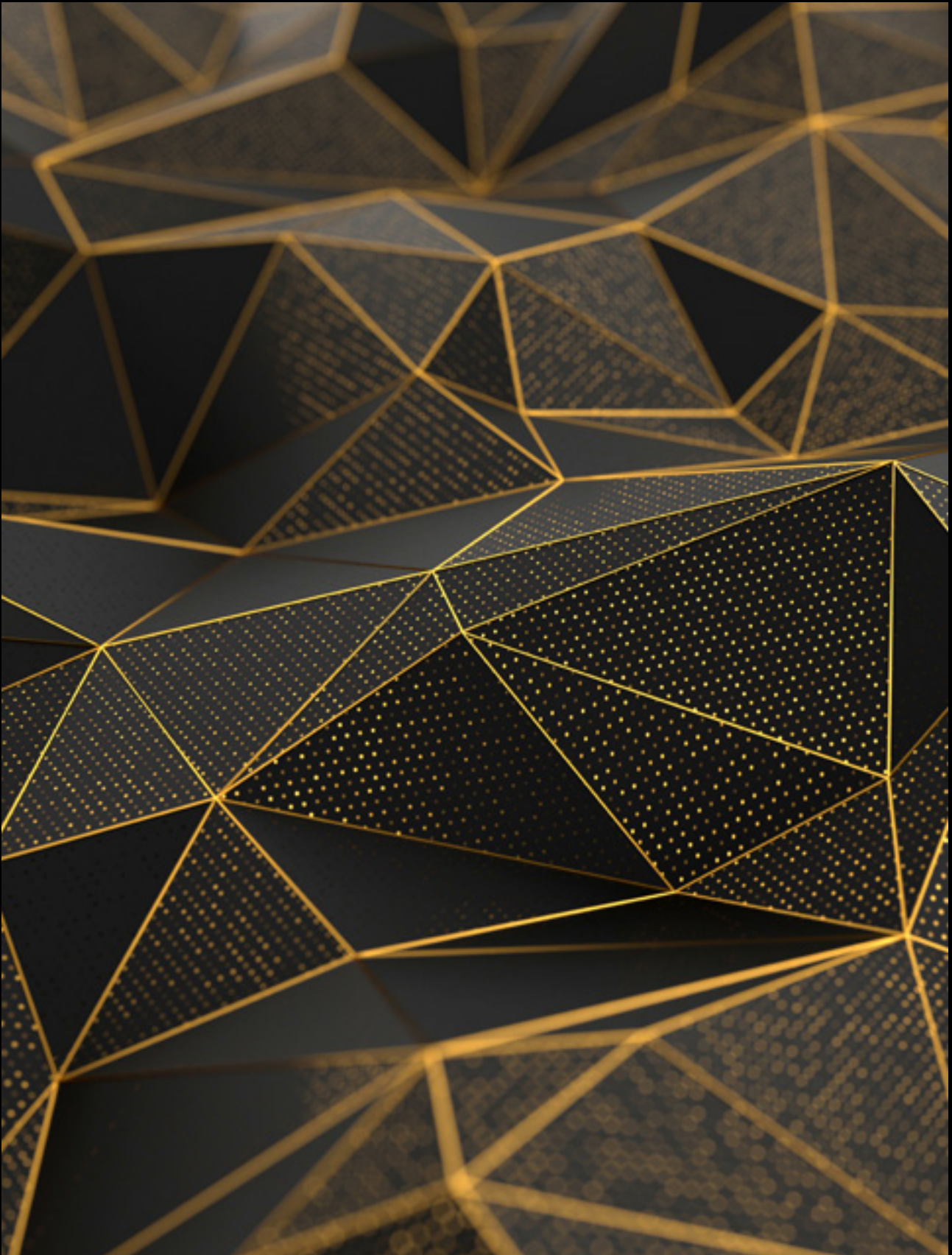
In doing so, institutions can draw upon their experience from the early stages of the crisis to find their optimal working model for remote working.

- **Reduced carbon footprint**

Remote working is beneficial for the environment and, in turn, good for business. Eliminating daily commuting will lead to less traffic and therefore a lower carbon footprint, which in turn would save millions of tons of greenhouse gases from entering the atmosphere. By including remote working guidelines in the business plan, companies can meet ambitious international climate goals and show to stakeholders that they are a responsible, environmentally aware and sustainable company which in turn positively influences clients' purchasing decisions.<sup>14</sup>

## CONCLUSION

Like many of the BigTechs<sup>15</sup>, we believe remote work is here to stay and will be a fundamental part of new working paradigms. Institutions that are keen to make it a permanent part of working life going forward should build upon the experiences accrued during the ongoing pandemic as they adapt to this new reality. New operating models should be built around greater flexibility and remote working to deliver enhanced value to clients and stakeholders. Access to new infrastructure and applications that facilitate remote working, alongside improvements to employees' digital skills and a shift in organizational culture will allow a wider use of remote working in a considered and managed fashion.



## NEARSHORE

The practice of locating services and people in a country or countries closely neighbouring your own, nearshore outsourcing today offers a range of benefits.

### BENEFITS

- **It lowers the cost of certain services.** A key reason why nearshore outsourcing initially became popular. Delegating a range of tasks to specialists in a nearby country with lower labour costs can significantly lower a firm's expenses.
- **Hiring talent at a competitive price.** Nearshoring countries can offer specialists with a higher education and at least several years of experience in the related field, but who are less expensive than employees in the home location.
- **Time-zones are closely aligned.** Nearshore outsourcing allows you to operate across locations within the same or similar time-zones. This has benefits in terms of communication, working hours and travel times.
- **Fewer cultural and language barriers.** If nearshoring to the closest country to your own, there will be less issues around cultural alignment, and language differences may be less of an issue.
- **Greater legal and regulatory alignment.** Nearshore outsourcing within a bloc like the European Union, for instance, means firms can take advantage of a greater harmonization of laws and regulations.
- **Entering a new market.** Nearshoring can also be a first step to entering and competing locally within a foreign market.
- **Lack of trust and perceived lower quality of work output.** Some business owners are reluctant to trust lower-cost companies in neighbouring countries on the basis that the quality of their work and delivery will also be lower.
- **Confidential information and sharing of sensitive data.** A nearshoring relationship will typically require the exchange of confidential information when delegating business processes. Companies that do not wish to share such confidential information may accordingly reject outsourcing; those firms working with sensitive client data will want to be even more cautious, as the sharing of such client data with entities – particularly those located outside the home market – may not be permitted.
- **A fractured team spirit.** Everyday interactions – small talk, coffee breaks, game nights or seasonal festivities – play a key role in fostering team unity, engagement and loyalty. If roles within a function are split across teams in different countries, these may be harder to achieve, if not actively undermined.
- **Project suitability.** Some business functions and activities lend themselves better to outsourcing than others. IT development or testing are usually suitable functions for nearshoring, for instance. However, creative tasks which require closer engagement and interaction with customers or stakeholders may prove more difficult to be outsourced.
- **Compromised communications and delivery.** Communication in-house will typically be cleaner and faster than with an outsourcing partner located in a different country. It may prove more challenging to sync-up project work and deadlines as a result.

### CHALLENGES

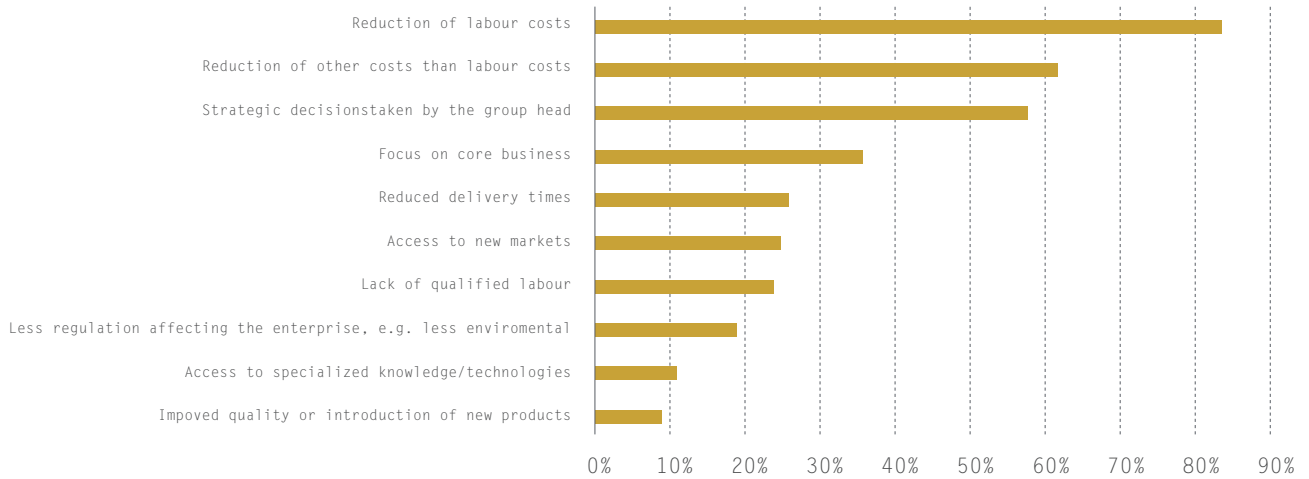
Despite the benefits that nearshore outsourcing offers, there are also some challenges to consider.

- **Higher costs than offshoring.** Although nearshoring may be less expensive than conducting business and software development operations in-house, it is usually not cheaper than offshoring to countries located further away.

### OUTSOURCING/NEARSHORING: CURRENT SITUATION BY THE NUMBERS

The following figure illustrates why companies are choosing the nearshore outsourcing model.

MOTIVATION FACTORS FOR INTERNATIONAL SOURCING ACTIVITIES (2014-2017)



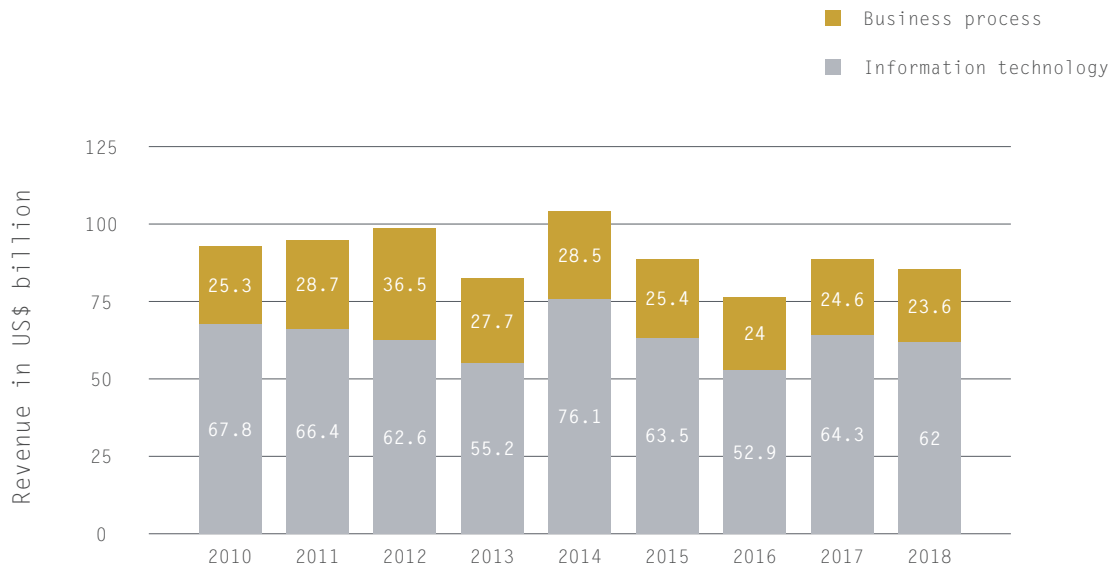
Source: Eurostat, SBS

Outsourcing has been popular across many different industries for decades. The most popular reason for outsourcing is cost-cutting. According to the European Commission’s latest International Sourcing (IS) study<sup>16</sup>, which gathered data from nearly 60,000 companies in 16 European countries for the period 2014 to 2017, reducing labour costs is the most popular reason for outsourcing, followed by the reduction of other costs and strategic decisions taken by the group head.

Interestingly, almost 40 percent of respondents said outsourcing meant they could put more focus on their core business, while a quarter outsourced specifically to access new markets or due to the lack of qualified labour. Less regulation abroad, access to specialized knowledge, improved quality or introduction of new products are less important factors for outsourcing activities. The conclusion seems that by outsourcing, businesses are rewarded with extra time and greater staff support; allowing them to scale, remain competitive, and (potentially) improve their services and offerings.

At the same time, financial services companies tell us they are feeling positive about their outsourcing relationships. Nearshoring has become a very popular outsourcing strategy, as the recent development of the global nearshoring market in business process and information technology shows.

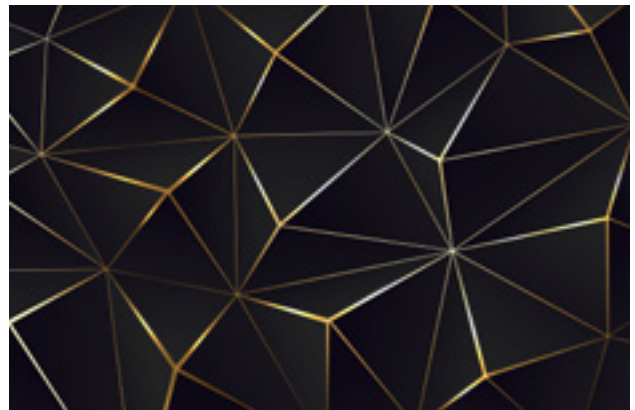
THE CHANGES IN GLOBAL NEARSHORING MARKET (2010-2018)



Source: Statista

As mentioned before, companies appreciate the possibility to arrange quick business travels, often without a need to organize visas or work permits. They enjoy that there is no difference in time-zones and smaller gaps in cultural habits while still the costs are lower as have it all in-house. Companies are usually engaging geographically close countries, so typically the US is nearshoring in Mexico or South America, while Western Europe is looking into the possibilities in Eastern Europe.

The following figure shows the top nearshore as well as offshore regions and their respective cost saving potential when outsourcing IT activities.



TOP NEARSHORE AND OFFSHORE LOCATIONS REGARDING OUTSOURCING OF IT ACTIVITIES



Source: MLSDev<sup>17</sup>

**CONCLUSION**

As we have established, remote working is set to be part of the new normal post-COVID. Nearshore working models have often been deemed unsuitable in the past, due to a perceived lack of control, trust issues or technological limitations. But in this new reality, where in-house employees themselves may be

working from home more frequently or even permanently, such reservations seem outdated. As noted, nearshore outsourcing can offer cost savings among other benefits. The current crisis is an opportunity for companies to re-evaluate their working models, and if properly scoped and implemented a nearshoring strategy can lower costs and enhance scalability and flexibility.

## OFFSHORE

True offshore operating models, relocating work to locations with high-quality talent pools but significantly lower labour rates such as India, the Philippines and China, are a well-established and proven business strategy. Government support programs and financial incentives, plus access to an educated workforce with good language skills mean many companies have been prepared to countenance potential cultural challenges, geographical distance and often major time-zone differences.

In the longer term, however, cost savings should not be the only consideration. There are multiple options open to firms looking to establish successful offshore models, ranging from a company-owned offshore service centre staffed by in-house employees, through joint ventures with established offshore service providers, to complete business processes outsourcing via external vendors.

The potential to achieve significant savings through offshoring has been widely regarded as easy to calculate. Nevertheless, there are many examples of how moving operations offshore did not deliver all the expected benefits – and sometimes even ended in complete failure. Below are some typical obstacles.

### CHALLENGES

- **Not all processes and activities are suitable for offshoring.** Thorough scoping of proposed offshoring activities is essential, and should begin with a thorough analysis of potential benefits and limitations, including the identification of business critical and non-business critical processes, the need for face-to-face contact and/or physical presence on the job.<sup>18</sup>
- **Underestimating the complexity of an offshore transition.** This can be difficult to evaluate in advance but drawing upon the knowledge and experience of offshoring specialists and external consultants will help planning and prioritization.
- **Managing regulatory and legal risks.** With offshore operations, it is key to fully understand all the regulatory and legal implications, and what specific obstacles or challenges may be involved.
- **Data safety regulations and governance.** The increased push for cross-border data protection over the past two decades (e.g. GDPR in the European Union, Cyberspace Administration of China) needs to be taken into account.
- **Increasing offshore costs.** One of the biggest drivers behind offshoring has been price. In the past, it was enough to have offshore centres in one location, which was growing over the time. Nowadays companies need to consider different geographical locations for increasing size of offshore centres, or setup smaller centres in multiple locations to mitigate dependency on local market situation.
- **Maintaining control, linking activities to objectives.** While offshoring is mostly used to reduce costs, implementations are not always as efficient as they might be. Proper goal setting and a robust business case at the outset will ensure a focus on the correct priorities and avoid distractions that do not support the primary objectives.
- **Managing cultural differences.** Collaboration across different countries requires employees to respect and be trained in cultural differences. Delivery deadlines, for instance, need to be given careful consideration to ensure alignment with local holidays and working practices.
- **Ensuring efficient communication.** Communications can be impacted by time-zones, cultural biases or different interpretations, and so the target audience, key objectives and realistic timeframes should all be front of mind when they are being drawn up and distributed.

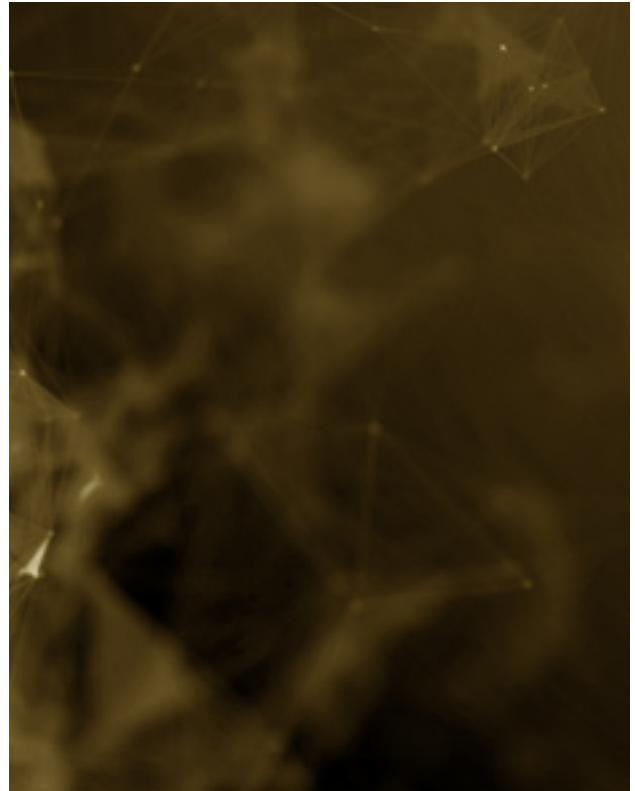
## BENEFITS

Offshoring has become for many financial institutions a vital part of their global operations strategy. Over and above costs savings, it enables additional team scalability, the ‘follow the sun’ principle can unlock 24/7 support options, the impact of geopolitical risks can be reduced and new cultural diversity can be injected into project teams.

## CONCLUSION

COVID-19 hit Asia without warning. Few predicted the subsequent global pandemic – initially was viewed as a local problem, like SARS during the previous decade. However, as the situation worsened globally, companies drew upon the experiences from APAC and swiftly implemented measures across other global locations and quickly updated business continuity runbooks. Maintaining a presence in different regions can not only help in the management and mitigation of local risks, but also be a source of valuable experience in difficult times.

What if another global crisis threatens financial institutions? During the current pandemic we saw humanity adapt at speed. People’s lives have changed, but the benefits of offshore remained the same: a cost-effective workforce supporting global operations.





## OUR RECOMMENDATION

As organizations look to reintegrate workforces post COVID-19, there is a clear recognition that alternate working models have both proved effective from a productivity perspective and offer the potential for cost savings. There are other benefits: improved job satisfaction, better work-life balance, enhanced task resourcing, the potential to attract previously untapped talent. Investing in a robust remote work infrastructure can also support new business opportunities by serving new clients currently not addressed and improving process efficiency, such as by transferring typical branch activities like the client advisory of complex products (e.g. mortgages) to a remote operations centre or home office, freeing up time for more sales.

**So, what is the right approach?** A hybrid operating model combining our four different options will in almost all cases prove the most effective approach. However, finding the right balance between them is a challenge, being dependent on individual operating models, technology infrastructures, the status of digitalization programmes, and organizational flexibility.

In general, we propose defining a reshoring strategy with a vision and actionable mission statement. There should be clear guidelines for the whole organization, detailing where an onsite presence is required, how remote working can be used, and whether nearshoring or offshoring are options. Existing business continuity plans must be reassessed, with particular attention paid to the potential future pandemics or other crises.

Clearly, not all the benefits of shoring can be realized right from the outset. Investment decisions need to be made accordingly, with an action plan and roadmap created, listing the required preconditions for success with clear deadlines and responsibilities for delivering them. The whole initiative must be complemented by a comprehensive change management plan, ensuring the whole organization is being included and supported on this journey.

## REFERENCES

1. <https://gartner.com/en/newsroom/press-releases/2020-04-14-gartner-hr-survey-reveals-41--of-employees-likely-to->
2. <https://newsroom.ibm.com/2020-05-01-IBM-Study-COVID-19-Is-Significantly-Altering-U-S-Consumer-Behavior-and-Plans-Post-Crisis>
3. <https://globalworkplaceanalytics.com/global-work-from-home-experience-survey>
4. John C. Maxwell, Teamwork makes the dream work (Nashville, Tenn.: J. Countryman, cop. 2002).
5. <https://forbes.com/sites/carolkinseygoman/2015/10/25/why-you-are-more-successful-in-face-to-face-meetings/#486a3f146315>
6. <http://uvm.edu/pdodds/files/papers/others/2004/kahneman2004a.pdf>
7. <https://ehjournal.biomedcentral.com/articles/10.1186/s12940-018-0427-5>
8. <https://wsj.com/articles/your-open-floor-collaborative-office-could-help-spread-coronavirus-11583784275>
9. <https://gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-survey-reveals-74-percent-of-orgs-to-shift-some-employees-to-remote-work-permanently>
10. <https://nber.org/papers/w26948.pdf>
11. <https://gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-survey-reveals-74-percent-of-orgs-to-shift-some-employees-to-remote-work-permanently>
12. <https://hcamag.com/asia/specialisation/mental-health/is-remote-work-creating-a-culture-of-presenteeism/223437>
13. <https://nber.org/papers/w18871>
14. <https://nielsen.com/us/en/insights/article/2018/sustainability-sells-linking-sustainability-claims-to-sales/>
15. <https://edition.cnn.com/2020/03/10/tech/google-work-from-home-coronavirus/index.html>
16. [https://ec.europa.eu/eurostat/statistics-explained/index.php/International\\_sourcing\\_and\\_relocation\\_of\\_business\\_functions#Motivations\\_for\\_international\\_sourcing](https://ec.europa.eu/eurostat/statistics-explained/index.php/International_sourcing_and_relocation_of_business_functions#Motivations_for_international_sourcing)
17. <https://mlsdev.com/blog/nearshore-software-development>
18. <http://princeton.edu/~blinder/papers/07ceps142.pdf>

---



# CYBERSECURITY

---

# CYBER PROGRAM DESIGN AND COMPLIANCE REVIEW

---

AUTHORS:

Julien Bonnay, US  
Jayadevan Vijayakrishnan, US  
Christopher Tecchio, US

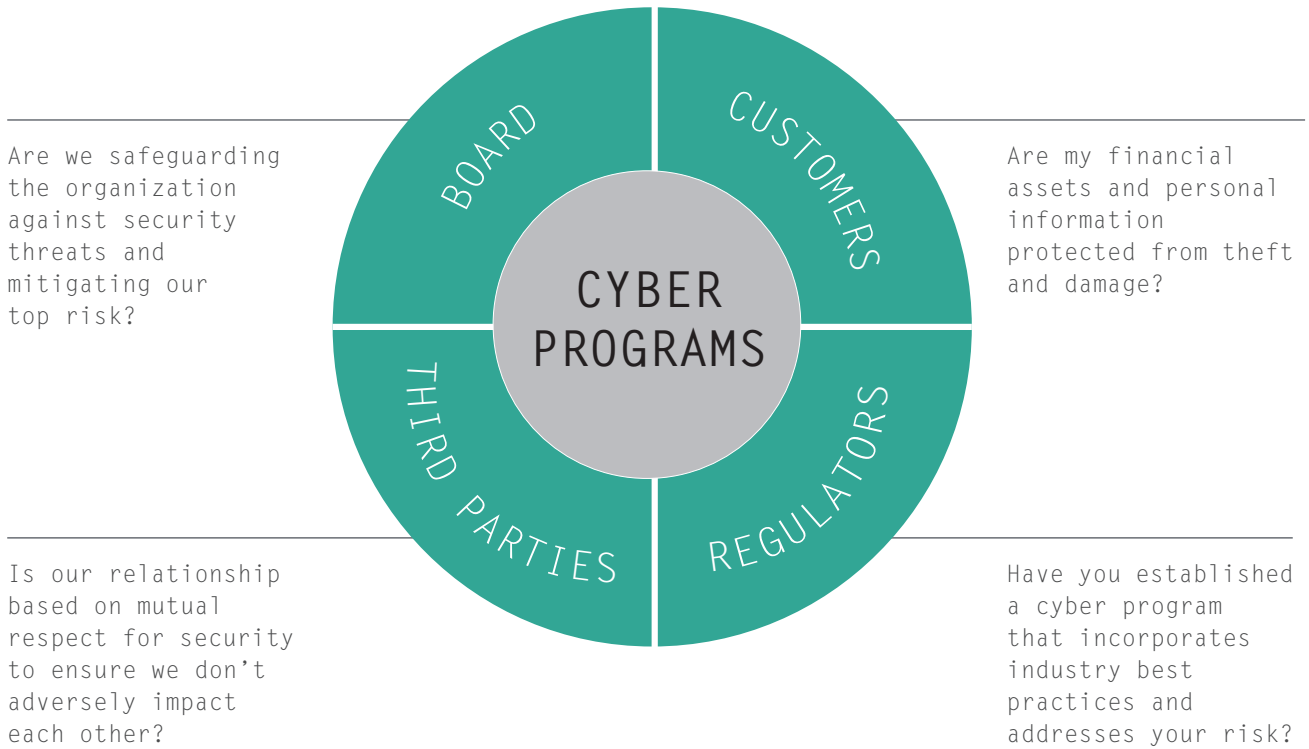
Cyber programs at financial institutions need to tackle the top cyber risks to the businesses, and address expectations of various stakeholder groups. Boards, customers, regulators, and third parties alike are increasingly looking for financial institutions to address cyber risks. As financial institutions contend with ever-increasing hacks and breaches, the Board is keen to ensure that the investments in cybersecurity are being directed to tackle the top cyber risks impacting the organization. Organizations have not only had to address concerns of their Board but in light of the recent spate of significant impact and highly visible data breaches, customers are also looking to their financial institutions to define effective cyber programs. In response to the crippling effect of many cyberattacks, regulators have also increased scrutiny on cyber programs, with bodies such as the New York State Department of Financial Services (NYDFS) mandating within the 23 NYCRR 500 regulation, a dedicated program to tackle cyber risk. On top of all these expectations, financial institutions also need to work as an ideal partner with third parties who could also be subject to adverse impacts resulting from any cyber risks.

“

*Designing a cyber program to enhance the organization's security posture effectively, entails defining strategic guiding principles that can be absorbed into the organization's standard operating procedures.*

”

EXPECTATIONS FROM CYBER PROGRAMS

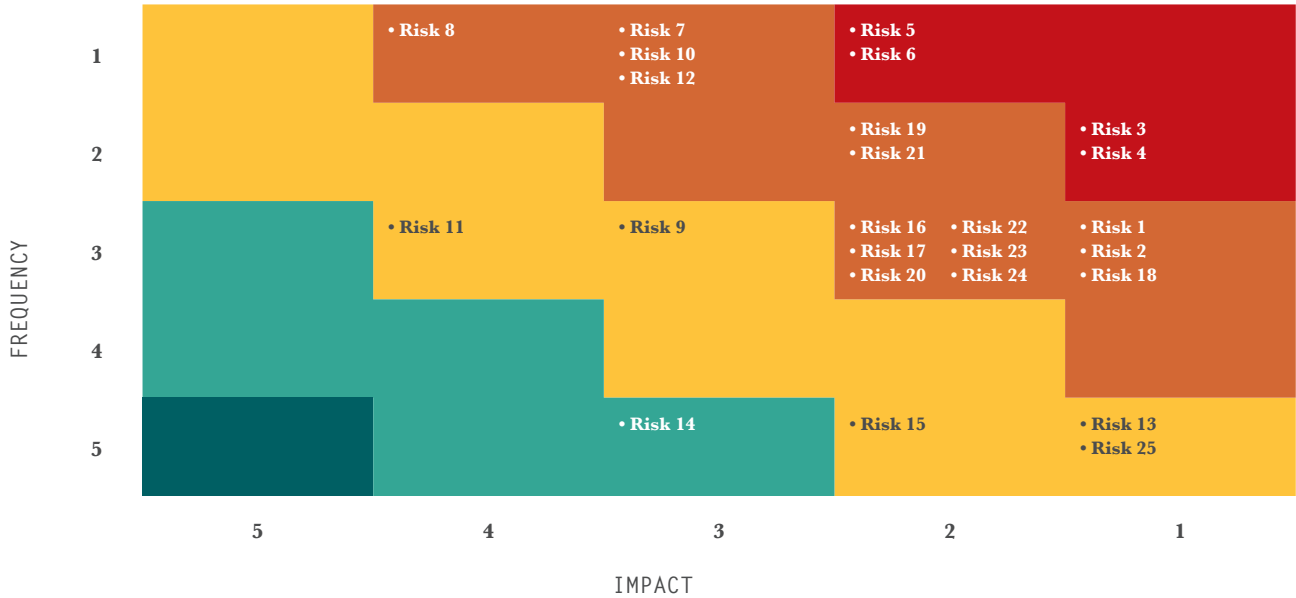


Cyber programs need to be comprehensive and address expectations from key stakeholders, as well as be supported by an effective compliance tracking mechanism. Further, cyber programs need to be treated at par with other enterprise risk programs and enforce a culture of continuous improvement. Capco follows a five-step approach to assisting Chief Information Security Officers (CISOs) at leading financial institutions define and deploy cyber programs.

**1. UNDERSTAND YOUR RISK PROFILE**

One of the prerequisites for any financial institution designing an effective cyber program is to build the cyber risk profile. This requires an organization-wide understanding of the critical business products/services, supporting processes, and underlying technology assets. An evaluation of the impacts to the organization caused by disruption to these products/services, processes, or underlying technology will help the organization define its cyber risk appetite. This risk appetite is an essential input into the design of a cyber program as it will help determine the maturity requirements for the program.

CYBER RISKS TO CRITICAL BUSINESS PRODUCTS/SERVICES

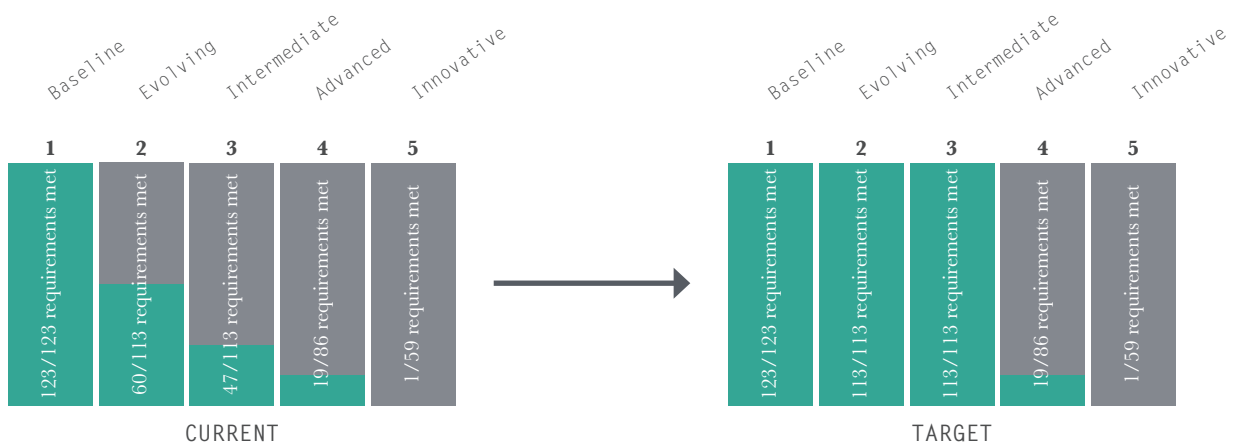


2. SET A REALISTIC TARGET

Setting an achievable target maturity helps determine the baseline requirements needed to build the cybersecurity program. To ascertain target maturity, organizations should conduct an assessment using a framework like the Cybersecurity Assessment Tool (CAT) from the Federal Financial Institutions

Examination Council (FFIEC) or the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST). Industry groups like the FFIEC and NIST have standards to help organizations align their cyber program's maturity with their risk profile.

SETTING TARGETS FOR THE CYBER PROGRAM

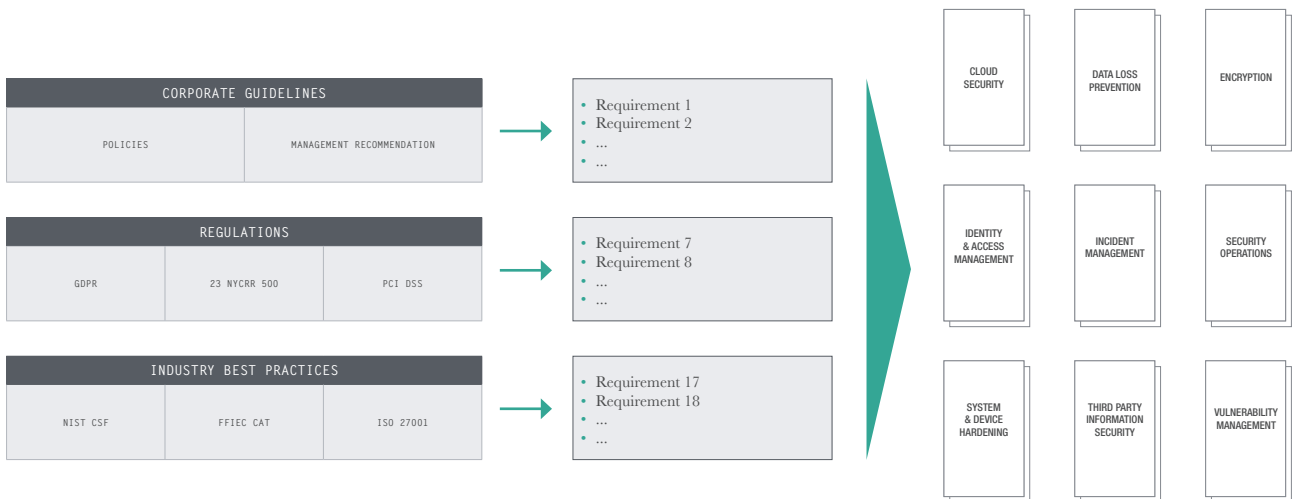


### 3. DEFINE ENTERPRISE STANDARDS FOR CYBER DISCIPLINES

Designing a cyber program to enhance the organization’s security posture effectively, entails defining strategic guiding principles that can be absorbed into the organization’s standard operating procedures (SOPs). The inclusion of the cyber requirements into SOPs has proven to be one of the best mechanisms to enforce security by design to be mandated across the enterprise. To build out the principles for these SOPs, organizations should take into consideration inputs from a variety of sources including policies and mandates set by management, applicable regulations, and industry best practices. These inputs can be leveraged to build

an inventory of requirements that will be the foundation of the cyber program. Using the results from the maturity assessment, the organization can choose the requirements that align with its target maturity to create a set of SOPs covering relevant cyber disciplines (e.g., Identity and Access Management, Security Incident Management, Encryption, etc.). Each SOP should have an owner accountable for ensuring that the included requirements will achieve the envisioned target state of the program. Further, these SOPs should be approved by senior management and published to a central depository for accessibility by all staff.

#### STANDARD OPERATING PROCEDURES FOR CYBER DISCIPLINES

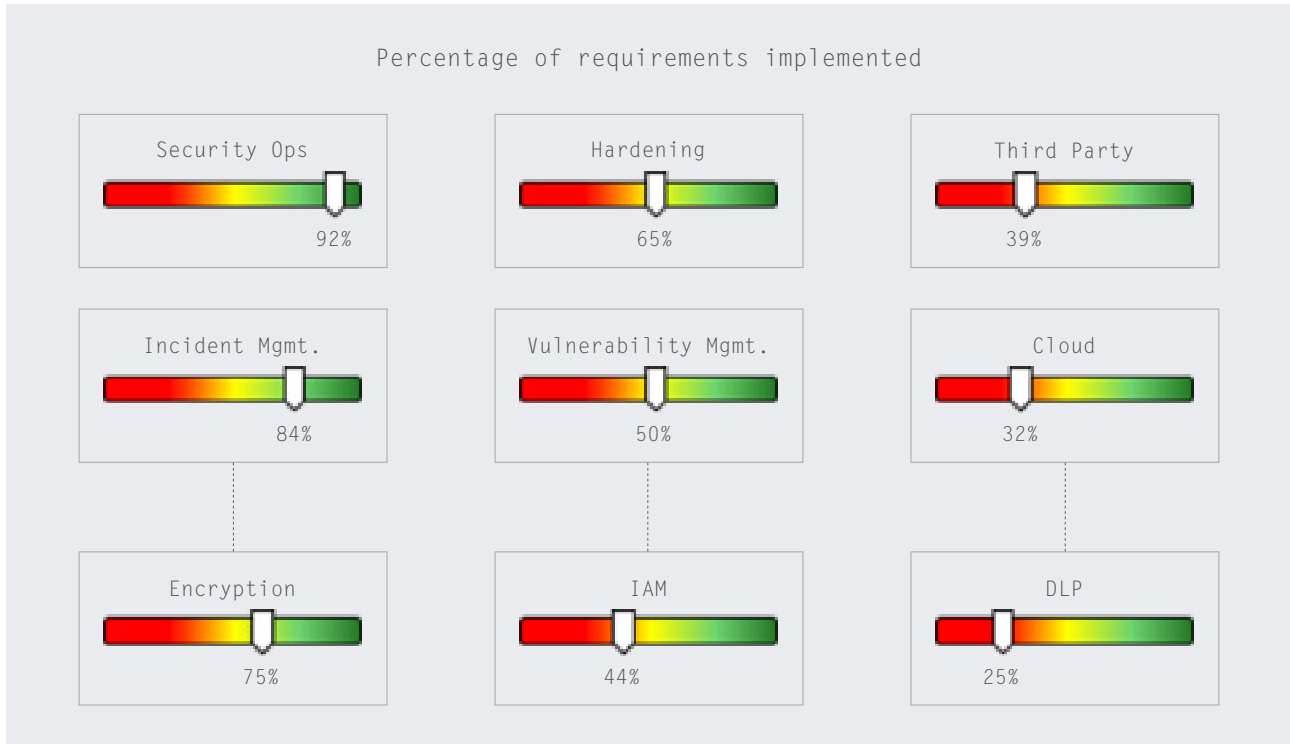


### 4. IDENTIFYING MATURITY AND COMPLIANCE GAPS

Once the SOPs have been defined, approved, and published, the organization should evaluate its current level of compliance with the requirements in the SOPs, and identify where gaps exist in achieving the program target. This can be accomplished in two phases. The first is an assessment conducted in coordination with information technology and information security management to gain an understanding of which requirements are already implemented, to what extent, and which are the most significant

gaps to current operations. This phase provides the organization with a high-level understanding of their current capabilities and problem areas. The second phase involves a detailed compliance review including the collection of supporting evidence. The results of these assessments will provide management and leadership teams with a heatmap of maturity challenges across the cyber disciplines and serve as an input into investment prioritization for remediation efforts.

## MATURITY AND COMPLIANCE GAPS

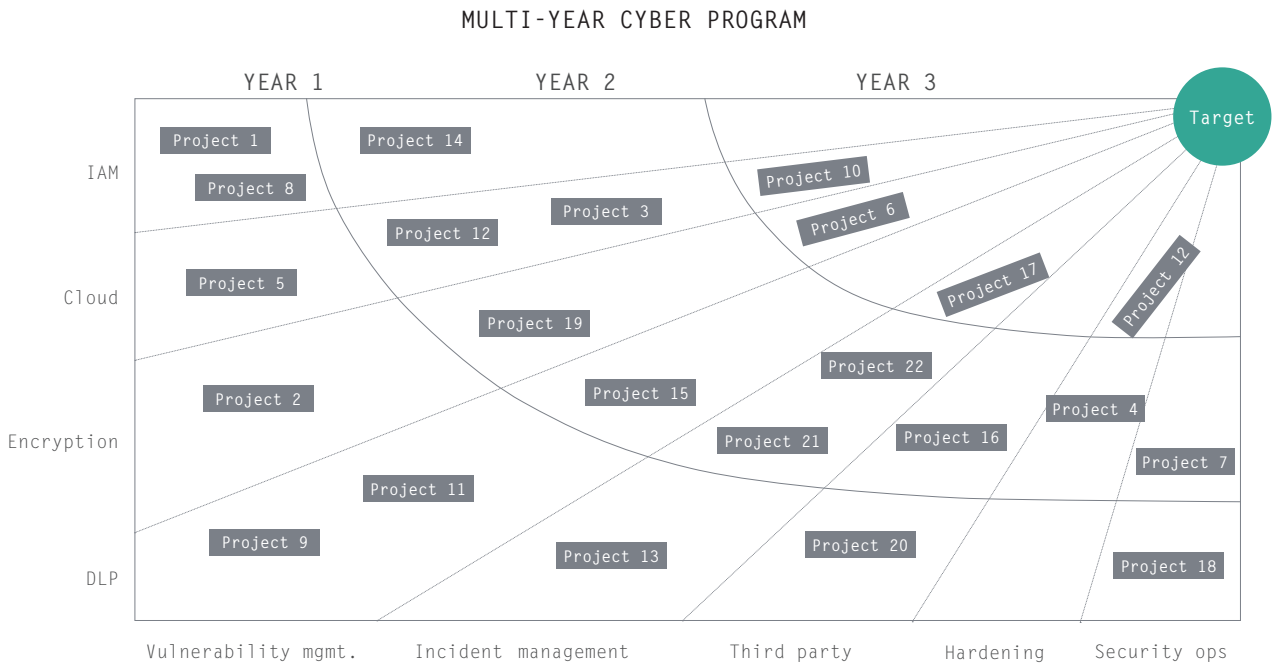


## 5. DEFINE A MULTI-YEAR CYBER PROGRAM

Often the remediation efforts to address gaps identified through the assessments will vary in size, cost, and complexity. Hence, defining a standard approach for planning remediation for the gaps is essential to the success of the program, though not always straightforward. Firstly, the gaps should be grouped together based on potential synergies to form more significant initiatives that can be examined for effort, scope, and cost. This will create a book-of-work that defines the scope of the remediation program for the next few years. The next challenge faced is determining which initiatives to address on priority and which can be deferred to the following years. Organizations should use a risk-based approach, recalling the effort performed earlier to

define the organization's risk profile, and prioritize according to the impact each initiative has on risks associated with critical business products/services, supporting processes, and underlying technology assets. Initiatives that help address regulatory compliance should also be considered at a higher priority. Once a priority is established, the organization can begin to build their roadmap while taking into consideration additional factors such as budget constraints, resource capacity, and management preferences. This roadmap will become a vital tool for achieving the target maturity established for the cyber program, providing structured transition periods for organizations to implement specific controls over time.

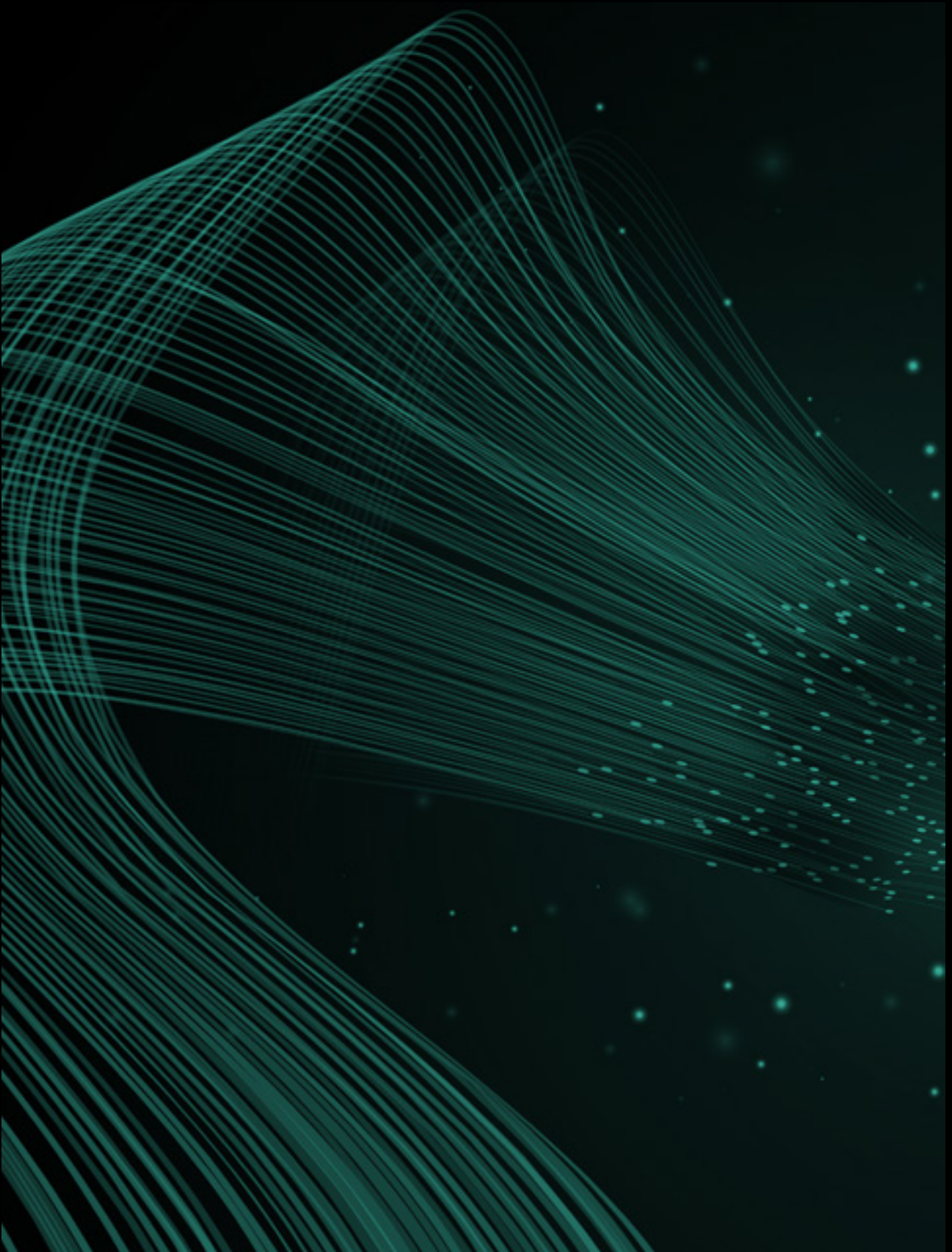




**SUCCESS FACTORS**

Attention to the following is an absolute must to ensure the continued success of cyber programs at financial institutions:

- Senior leadership buy-in and sponsorship of the cyber program drives a culture of the rapid adoption of industry best practices.
- Non-technical aspects of cybersecurity such as business cyber risk identification, governance, incident communication, etc. deserve equal consideration to the technical components.
- Single point of ownership for the SOP for each cyber discipline is critical to building accountability.
- Definition of KRIs and metrics are crucial to tracking the effectiveness of the cyber program as well as providing visibility for management.
- An annual refresh of the cyber program is essential to maintain the program current and address top cyber risks, management expectations, and relevant regulations.



# FIVE CYBER SECURITY TRENDS IN 2020

---

AUTHOR:  
Julien Bonnay, US

The need for cybersecurity in the financial services industry has never been greater. Financial institutions (FIs) have been and will continue to be the subject of cyberattacks by adversaries of all varieties. The old adage “why do you rob banks....because that’s where the money is” holds in this domain as well. In 2019, 86 percent<sup>1</sup> of breaches were financially motivated, and the records exposed in all breaches increased by 284 percent<sup>2</sup>. And if that’s not enough for FIs to worry about, consider that the average cost of a breach as disclosed by public firms in 2019 was \$116 million<sup>3</sup>. Given the magnitude of this issue, we have listed the top trends we gleaned from our client work in 2020.

“

*An expanding talent gap and rapid growth of cybercrime are trends that will continue for some time.*

”

## CRIME DOES PAY, ON THE DARK WEB, THAT IS

Projections are that cybercrime will exceed \$6 trillion annually by 2021 up from \$3 trillion in 2015<sup>4</sup>. Probably the most significant factor driving this acceleration is the increasing efficiency of cybercriminals. The dark web has become a thriving black market where criminals of all means can gain the capabilities necessary to launch sophisticated cyberattacks. Gone are the days when attackers needed significant skills to launch an attack. In many ways, the dark web has commoditized attack tools while also providing a means of trading the spoils of an exploit. With Bitcoin and a Tor Browser, a would-be attacker, now has access to a plethora of malicious capabilities that include ransomware as a service, botnets for rent, and malware as a service, to name but a few. Given lowering barriers to entry and the financial payoff, expect cybercrime to continue rapid acceleration.

## IT'S GOOD TO HAVE INTELLIGENCE

As most FIs have realized, cyber threat intelligence is a critical component of a successful cyber program. Understanding adversary behavior and tendencies can help a firm anticipate and react quickly before or shortly after an attack. Many firms have instituted 'Cyber Fusion Centers' to facilitate this interaction. That said, significant challenges exist in operationalizing intelligence in a way that prioritizes activities for cyber defenders. A significant problem is the sheer volume of data available from multiple sources and the challenges associated with culling it into actionable intelligence to inform defensive processes such as attack surface reduction, detection logic creation and red team scenarios. Add to this the fact that security and orchestration technologies in existence today typically do not integrate well. Going forward, we expect continued emphasis on developing the next generation Cyber Fusion Center to extract value from cyber threat intelligence in a more streamlined and efficient manner.

## THE CLOUD MAKES LIFE EASY

Unfortunately, benefits can also accrue to those with nefarious intent – firms are moving to the cloud at an amazing clip and with good reason. Higher efficiencies, quicker speed to market and many enhanced capabilities drive up demand. Additionally, underlying cloud infrastructure can be more secure than legacy infrastructure thanks to additional attention paid by the cloud vendors as well as a consolidated and integrated approach. That said, there are pitfalls from a cybersecurity perspective. Chief among them is the need for comprehensive security solutions that incorporate the cloud as well as legacy infrastructure. Given the shortage of cloud security expertise and the lack of hybrid solutions that span cloud and legacy, companies are challenged to build in system-wide security. Also, due to the consolidation effects of the cloud, small errors in misconfiguration can have devastating consequences, as demonstrated by many recent breaches. Expect to see both increasing use and misuse of the cloud driving up the need for talent and integrated cloud security solutions.

## YOU HAVE TO BE AGILE TO SURVIVE

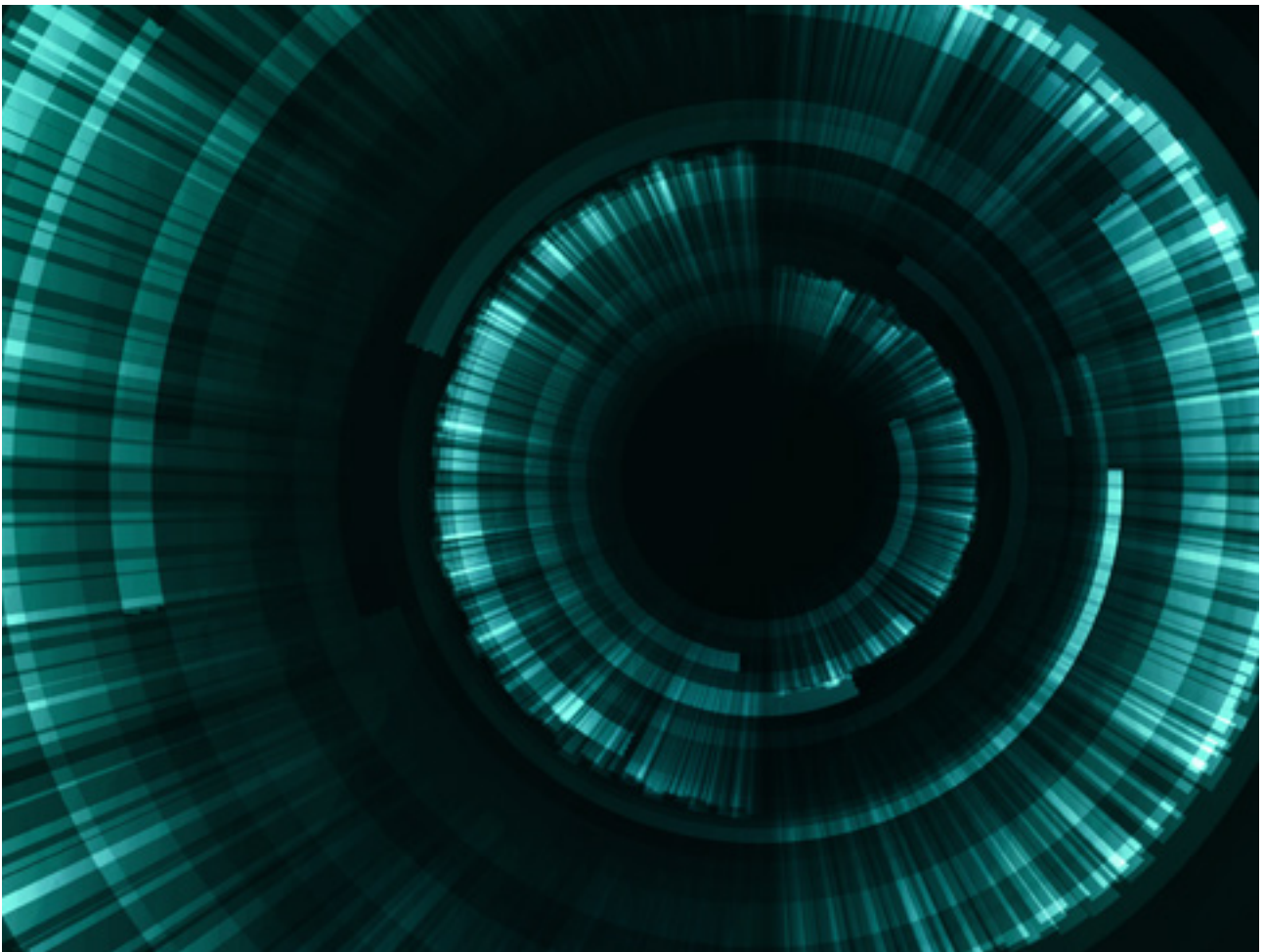
Today's customers are demanding the ability to transact fully and securely in the digital domain and competitors are offering new choices daily. FIs are realizing that keeping up in today's world of rapid digital transformation means adopting agile development. When done well, agile allows FIs to keep up with the rapid pace of technological change; however, building security into the process presents a whole new set of issues. Characteristics of agile development include small teams working quickly and iteratively, where you don't write requirements down, design and risk decisions are made just in time, and manual testing and compliance can't keep up with the speed of delivery. Clearly, our traditional waterfall approaches to building security can't keep up. To be successful, agile teams need a deeper understanding of security issues, willingness to adopt security practices, and must take increased responsibility for the security of their systems. In addition, security professionals need to work faster, more iteratively, and learn to view cyber risk and mitigations in more incremental terms. While all of these changes are possible, success often requires changing deep-rooted cultural drivers and incentives. It will not happen without a clear plan as well as an organizational commitment at all levels. Expect the transformation to secure agile development to remain a top issue for some time to come.

## PEOPLE, ALL YOU NEED IS PEOPLE

According to ISC<sup>2</sup>, the number of unfilled cyber positions now stands at 4M professionals<sup>5</sup> world-wide. Add to this the fact that, according to the 2020 Verizon Data Breach report, nearly half all cyber incidents in financial services can be attributed to actions conducted by people. Clearly, we have a significant people issue. We fully expect our clients to continue to reach for assistance in finding qualified staff and training up the staff already on board.

## WHAT THE FUTURE HOLDS

Going forward, it is clear that several factors are converging to increase cyber risk for FIs. Market forces continue to push FIs to rapid and comprehensive digital transformation, accelerating the use of technologies such as the cloud and agile and increasing exposure to the many inherent security issues. Moreover, the combination of an expanding talent gap and rapid growth of cybercrime are trends that will continue for some time to come. FIs that invest in technologies and processes such as cyber fusion centers, secure cloud, secure agile and cyber talent development can greatly reduce cyber risk and significantly increase the probability that adversaries look elsewhere to exploit easier targets.



## REFERENCES

- <sup>1</sup> [Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexander Pinto, Suzanne Widup. “2020 Data Breach Investigations Report” \(Verizon 2020\)](#)
- <sup>2</sup> [Inga Goddijn, Executive Vice President, Risk Based Security. “Risk Based Security, 2019 Year End Report, Data Breach QuickView” \(Risk Based Security 2020\)](#)
- <sup>3</sup> [Audit Analytics. “Trends in Cybersecurity Breach Disclosures, May 2020”](#)
- <sup>4</sup> [Steve Morgan, Editor-in-Chief, Cybersecurity Ventures. “2019 Official Annual Cybercrime Report” \(Herjavec Group, 2019\)](#)
- <sup>5</sup> [ISC<sup>2</sup>. “\(ISC<sup>2</sup>\) Cybersecurity Workforce Study, 2019, Strategies for Building and Growing Strong Cybersecurity Teams.” \(ISC2, 2019\)](#)

---

## ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

## WORLDWIDE OFFICES

Bangalore	Geneva	Paris
Bangkok	Gurgaon	Pune
Berlin	Hartford	São Paulo
Bratislava	Hong Kong	Singapore
Brussels	Houston	Toronto
Charlotte	Kuala Lumpur	Vienna
Chicago	London	Warsaw
Dallas	Mumbai	Washington, DC
Dusseldorf	Munich	Tysons Corner
Edinburgh	New York	Zurich
Frankfurt	Orlando	

---

**CAPCO.COM**







**CAPCO**