COVID-19 Business Briefing

Updated Edition

Banking
May 2020

pwc

Foreword

Roxane Haas, Banking Industry Leader

Dear Business Leaders,

At this time of uncertainty, the focus of governments and, indeed, the wider world is on the immediate health crisis that COVID-19 represents. This phase will eventually come to pass as vaccines are developed and we adjust to the unprecedented shift that we are facing.

In the context of the COVID-19 outbreak and its global spread since February, financial regulators have taken a string of measures to help firms mitigate the crisis. **The Luxembourgish regulators were among the first to provide clear guidelines** in order to guarantee both operational continuity and adequate safety level of the workforce. The instructions enacted specifically for banks ensured the maintenance of not only high-quality services but also customers protection levels, providing flexibility and allowing markets to function smoothly.

The banking sector is addressing the current emergency situation from a completely different standpoint than the global financial crisis of 2008. In recent years, banks have consistently strengthened their financial positions, reduced exposure to non performing loans, improved their capital ratios and accumulated liquidity buffers to cope with crisis situations like this. Unlike in 2008, banks are not seen as a trigger element of the crisis but are considered a fundamental part of the solution.

As close observers of the European financial sector, we believe that **Luxembourg banks have been particularly prompt to inject new credits into the markets and the real economy**. **Private banks and Asset servicers have been, on their end, particularly agile in adapting to the new environment by deploying Home Based Working, adapting internal controls, answering incoming requests and ensuring continued service levels to clients.**

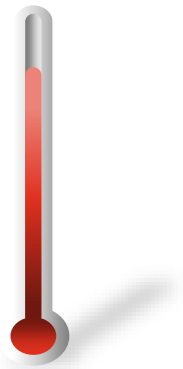
To help the banking sector in this unfolding situation, we at PwC Luxembourg have put together a document highlighting the key points where we believe your focus should be: which regulatory or environmental changes will have the most impact on your bank, will these be a risk or a relief, and how should you approach these impacts on your business. Our attention dashboard highlights the dimensions which are most significantly impacted by the crisis: Financial Impact; Operations and Data; Regulatory, Risk & Compliance; as well as Client Relationship.

Although your current attention may be on handling the COVID-19 challenges faced by your bank, we highly encourage you to start looking beyond the crisis and evaluating how you can utilize current opportunities to be best positioned in a post COVID business environment.

During this time, our focus at PwC remains on our clients and the individuals listed in the contacts section remain at your disposal should you have any questions or need to discuss any of the points.

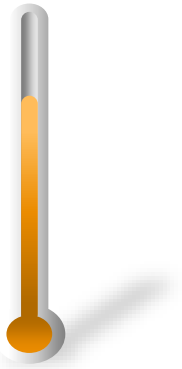
Kind Regards,
Roxane Haas

Management attention dashboard



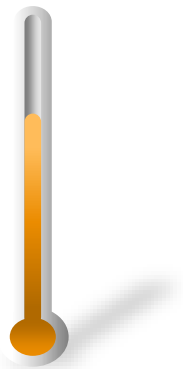
Financial Impact

- CREDIT DEFAULT RISK
- INTEREST RATE RISK
- LIQUIDITY RISK
- MARKET RISK CAPITAL REQUIREMENTS
- IFRS9
- MARKET VOLATILITY
- ECONOMIC RECESSION



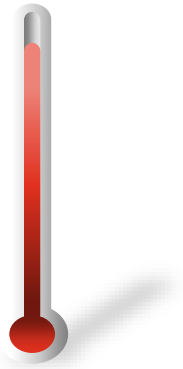
Operations & Data

- BUSINESS CONTIUNITY
- IT CAPACITY RISK
- CYBER SECURITY RISK
- SUPPLY CHAIN RISK
- WORKFORCE
- WORKPLACE



Regulatory & Compliance

- AML RISK
- DIVIDEND DISTRIBUTIONS & SHARE BUYBACKS
- PERMANENT ESTABLISHMENT UNDER BEPS
- DAC6
- REPORTING & DISCLOSURES
- STRESS TESTS
- BASEL III FRAMEWORK

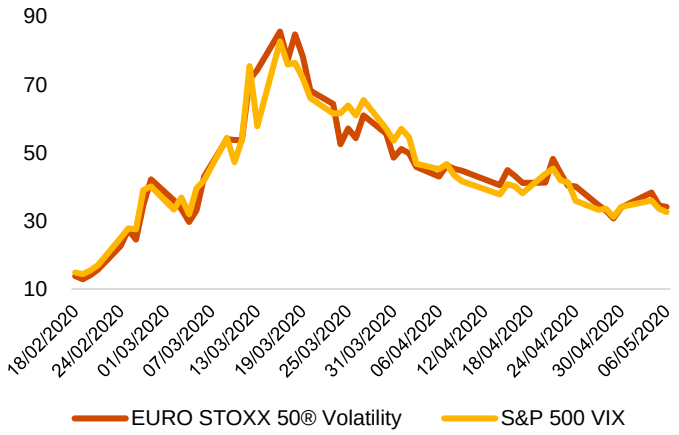


Client Impact

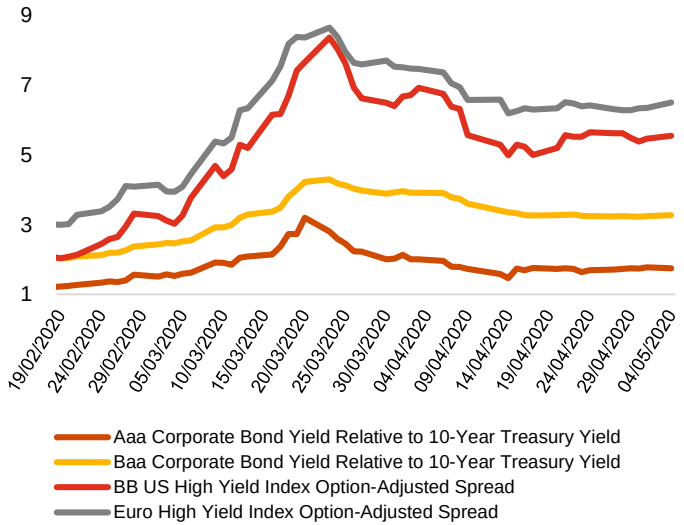
- GUARANTEED LOANS
- BRANCHES / ATMs
- CONSUMER PROTECTION
- PHISHING & ID THEFT
- HIGHER CUSTOMER EXPECTATION

Market dashboard

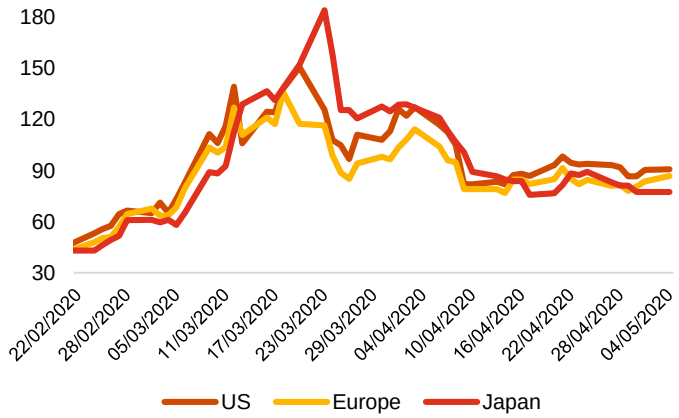
Equity market volatility indices



Euro and US Corporate bond yield spread in %



Corporate CDS spread, 5Y Investment grade



10-year government bond yield spread across selected economies as of 6 May 2020

Country	Yield	Vs Bund	Vs T-Note	2w variation
Austria	-0.115	43.7	-79.1	-20.8%
Belgium	0.033	58.4	-64.4	-18.8%
Canada	0.615	102.2	-0.9	5.0%
France	0.118	52.8	-50.3	16.2%
Germany	-0.407	0	-103.1	14.5%
Italy	1.89	244.2	121.4	-15.2%
Japan	-0.015	53.7	-69.1	-1.3%
Netherlands	-0.272	28	-94.8	-16.7%
Spain	0.872	142.3	19.6	-18.3%
Switzerland	-0.559	-0.8	-123.5	-16.7%
United Kingdom	0.218	76.9	-45.9	-10.9%
United States	0.676	122.8	0	5.2%

Sovereign CDS 1-month change as of 6 May 2020

Country	S&P Rating	5Y CDS	1m variation	Default Probability
Denmark	AAA	14.5	-13%	0.2%
Sweden	AAA	16.0	-6%	0.3%
Norway	AAA	17.0	6%	0.3%
Netherlands	AAA	18.8	2%	0.3%
Austria	AA+	20.3	-2%	0.3%
USA	AA+	20.5	12%	0.3%
Finland	AA+	20.5	-1%	0.3%
Singapore	AAA	20.7	-15%	0.3%
Germany	AAA	23.5	-2%	0.4%
New Zealand	AA	30.0	-23%	0.5%
Japan	A+	32.1	-24%	0.5%
Canada	AAA	33.0	0%	0.6%
UK	AA	33.5	-14%	0.6%
South Korea	AA	35.3	-8%	0.6%
Belgium	AA	40.9	2%	0.7%
Hong Kong	AA+	41.6	3%	0.7%
Ireland	AA-	42.4	-6%	0.7%
France	AA	45.9	12%	0.8%
China	A+	49.8	-13%	0.8%
Slovakia	A+	52.1	4%	0.9%
Poland	A-	62.4	1%	1.0%
Qatar	AA-	65.0	0%	1.1%
Croatia	BBB-	77.0	-2%	1.3%
Israel	AA-	77.1	-10%	1.3%
Philippines	BBB+	85.0	-21%	1.4%
Chile	A+	100.1	-31%	1.7%
Malaysia	A-	109.9	-7%	1.8%
Portugal	BBB	119.9	14%	2.0%
Spain	A	120.4	11%	2.0%
Russia	BBB-	158.9	-4%	2.7%
India	BBB-	209.5	-11%	3.5%
Indonesia	BBB	215.9	-13%	3.6%
Colombia	BBB-	217.4	-6%	3.6%
Italy	BBB	221.0	19%	3.7%
Mexico	BBB	228.5	-9%	3.8%
Bahrain	B+	255.0	0%	4.3%
Greece	BB-	263.3	15%	4.4%
Brazil	BB-	317.4	-10%	5.3%
South Africa	BB-	406.8	-15%	6.8%
Turkey	B+	585.7	-9%	9.8%
Pakistan	B-	595.7	-14%	9.9%
Ukraine	B	635.7	-9%	10.6%
Egypt	B	635.9	15%	10.6%
Argentina	SD	13134.1	58%	100.0%

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
Credit default risk	On 25 March, the European Banking Authority (EBA) has released a statement on applying the prudential framework regarding Default, Forbearance and IFRS9 in light of measures to manage the COVID-19 pandemic. The statement provides clarity for the banking sector on how to handle in a consistent way certain elements relating to: (i) the classification of loans in default; (ii) the identification of forborne exposures; and (iii) the accounting treatment.	✓ Credit quality may quickly deteriorate, especially in sectors that are hit the hardest by the lockdown. This situation may overwhelm existing impairment models, requiring more resources to assess the impact of changing market conditions. It could have an effect on stress-testing in general.	✓ Begin a detailed review of your credit portfolio as soon as possible to assess how the situation will affect credit quality. Make sure that your key assumptions (your own or those developed by external service providers) are still valid, and that the qualitative reserves you've identified still make sense. While the situation is evolving quickly, you may want to adjust economic scenarios or the associated weighting of such scenarios within your modelling.	RISK	HIGH
Interest rate risk	Prior to the COVID-19 pandemic, interest rates were already at a historical low. As confinement measures were swiftly implemented in Europe and the US, global central banks announced further interest rate cuts to try and calm down market volatility.	✓ In this economic context, the levels of interest income are even lower than forecasted. This fact, combined with increased margin pressure, will have serious consequences on the profitability of banks.	✓ Conduct a comprehensive analysis of the impacts of protracted low interest rates in this economic environment, in particular related to the asset-liability management process. ✓ Scenario analysis is essential in times of interest rates uncertainty.	RISK	HIGH
Liquidity risk	While the ECB currently allows banks to breach their LCR ratios, it is important to keep in mind that the CSSF requires contingency plans to be implemented and periodically tested, so as to ensure any applicable liquidity management tools can be used in a prompt and orderly manner when necessary.	✓ Given rapid changes in banks' operations, current liquidity risk tools and measures could be outdated. ✓ Interbank exposures may also have a strong impact on banks' balance sheets.	✓ Any shortcomings in liquidity management tools emerging as a result of the COVID-19 pandemic should be addressed immediately. ✓ Actions to take regarding interbank exposures include closely monitoring liquidity, transaction volumes, term length and interbank rate of lending market, as well as assessing counterparty risk through scenario analysis.	RISK	HIGH

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
NEW **Market risk capital requirements**	On 16 April, the ECB announced that it is temporarily reducing a supervisory measure for banks – the qualitative market risk multiplier – which is set by supervisors and is used to compensate for the possible underestimation by banks of their capital requirements for market risk. On 22 April, the EBA issued a statement on the application of the prudential framework in the area of market risk during the COVID-19 outbreak. This statement covers four areas: ▪ mitigation of the increase in aggregated amounts of Additional Valuation Adjustments (AVAs); ▪ postponement of the Fundamental Review of the Trading Book under the Standardised Approach (FRTB-SA) reporting requirement; ▪ postponement of final two implementation phases of the margin requirements for noncentrally cleared derivatives; ▪ increase in the Value-at-Risk (VaR) risk metrics and multiplication factors under the Internal Models Approach (IMA) for market risk.	✓ The EU prudential regime related to market risk monitoring and capital adequacy is very sensitive to financial market volatility. As a result, banks will need to closely monitor prudential ratios in order to meet economic, regulatory and rating agency capital requirements.	✓ Addressing the ability to respond effectively to regulatory requests for information. ✓ Determine whether the process established to control and adapt to changes in monitoring requirements is sufficient. ✓ Consider the comments required by the statutory auditors on the adequacy of the regulatory reports to be issued, including subsequent events and interim results.	RELIEF	HIGH
NEW **IFRS 9**	On 20 March, the ECB recommended that institutions: ▪ opt to apply the transitional IFRS9 provisions foreseen in the Capital Requirement Regulation (CCR); ▪ avoid excessively procyclical assumptions in their IFRS9 models to determine their provisions. On 14 April, the CCSF issued further guidelines on how banks can use the flexibility allowed by the IFRS 9 accounting framework, answering the two following questions: ▪ how should banks address the procyclicality in IFRS9? ▪ is the application of the IFRS9 transitional arrangements necessary and when should a bank apply for it?	✓ The ECB recommendations aim to mitigate volatility in institutions' regulatory capital and financial statements stemming from IFRS 9 accounting practices in the current context of extraordinary uncertainty. ✓ However the CSSF emphasizes that banks should continue to apply sound and prudent risk management, in particular with respect to the potential crystallization of COVID-19 related risks. In particular, the CSSF recommends to monitor the deterioration of borrowers' creditworthiness (beyond COVID-19 related, purely short term transitional impacts).	✓ Banks are required to monitor key financial statements metrics (forbearance and non performing exposures, expected credit loss) and regulatory metrics (solvency) under the assumption that the flexible treatment for such exposures is no longer warranted. ✓ Consider the comments required by the independent experts on the adequacy of the financial statements to be issued.	RELIEF	HIGH

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
Market volatility	On the positive side, some banks are taking advantage of the situation, with market volatility generating higher volumes of trading thus leading to increased broker and trading fee income. On the negative side, volatility limits the effectiveness of hedging strategies, impairs the validity of valuation processes, and may impact the bank's trading portfolio.	✓ Some banks may have high exposure to sectors at risk during the crisis (travel, leisure, construction, etc.). ✓ Banks may not have the right level of provisions due to higher expected losses in banking book under IFRS9. ✓ Private banks with Lombard loans may be impacted through margin calls.	✓ Actions to take regarding the trading portfolio: re-evaluate securities; assess potential impairment needs. ✓ Actions to take regarding the loan portfolio: identify affected assets quickly; monitor COVID related measures (i.e. payment deferrals, interest rate adjustments, public guarantees), and conduct rapid scenario analysis review of loan portfolios.	RISK	MEDIUM
Economic recession	The recent stop of economic activities has driven a decrease in consumer confidence and a huge drop in consumption, followed by a fall in stock prices and cash flow forecasts. All these elements have increased the risk for a potential global recession.	✓ Negative consequences on several balance sheet and profit & loss items, including the credit portfolio.	✓ You may find that you need to reassess a wide range of financial models and analyses for the current environment. ✓ The cost of switching suppliers may impact your bottom line forecasts. ✓ The lack of demand for certain products or services may prompt you to review your business plan.	RISK	MEDIUM

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
UPDATED **Business continuity**	Business continuity plans have had to be implemented to maintain operations. On 12 March, the CSSF noted that "supervised entities started to implement their business continuity plans (BCP) by deploying the means deemed necessary." On 22 March, the CSSF called for supervised entities to ensure that "where staff is not equipped with laptops or other mobile devices, entities implement as soon as possible virtual desktop and other remote access solutions, cloud based or not."	✓ The majority of banks have successfully put their BCP to the test in recent weeks. However, these plans typically do not take into account disruptions across multiple operational lines at the same time and the ripple effect that the current situation is having on global supply chains and markets. ✓ Most business continuity plans did not foresee the situation of lockdown and near full home-based working. ✓ Health impact on staff working from home, or at work under strict social distancing measures, should not be underestimated.	✓ Maintain regular connection with staff and clients. ✓ Reinforce ability to monitor operations and performance on a real-time, remote basis. ✓ Prepare detailed plan for progressive deconfinement and ensure the safety of staff and clients. ✓ Plan for "second wave" pandemic or resurgence of COVID-19. ✓ Consider re-assessing the enterprise wide risk management framework. Review outsourced services and inherent processes across the whole value chain.	RISK	MEDIUM
UPDATED **IT capacity risk**	Technology related infrastructure was already under considerable strain in many companies. The deployment of Home Based Working (HBW) measures allowed for potentially a high number of employees to access core systems remotely with a raft of questions around sufficiency of professional mobile devices, connection bandwidth, adequacy of mobile phone packages, etc. Certain business have suffered with legacy infrastructures. On 23 March, the CSSF informed that supervised entities may opt for cloud-based solutions in response to the Covid-19 situation (prior authorisation or notification to the CSSF is not required as long the current situation lasts).	✓ Difficulty in maintaining normal capacity levels, and accessing core IT platforms on a remote basis, especially for businesses not cloud based. ✓ Some entities had to acquire new portable hardware to enable staff to continue to work. ✓ Internet lines VPN saturation put pressure on bandwidth levels but also on the servers; endpoint (VPN servers) capacity issues; VPN licenses number too limited; applications not ready to work remotely (security,...).	✓ Continue to organise appropriate IT support presence on site (different teams, shift management, etc.). Enable the service desk to support remotely . ✓ Organise load testing of the VPN (BCP approach); make sure VPN licenses are aligned with the number of employees. ✓ As part of the return to normal, some entities may implement shifts or allow employees to work early/late hours, which means that applications will have to be accessible over longer time periods. This may have an impact on night back-ups and batches. ✓ Consider cloud-based tools and solutions. ✓ Plan for "second wave" pandemic or resurgence of COVID-19.	RISK	MEDIUM
UPDATED **Cybersecurity risk**	Cybersecurity is a major issue in the financial sector, and a top priority for regulators. Phishing and online fraud attempts are increasing, with criminals that are taking advantage of the current emergency situation related to the outbreak of COVID-19. When thinking of HBW, most of the companies didn't prepare for this scale of adoption and for such a long time period. The current situation allows for less restrictions, with uncertainty on the way personal computers are stored and whether security due diligence processes are performed.	✓ Banks' infrastructure had not been tested for security loopholes, thus giving rise to risks for data protection and data security that should not be underestimated. ✓ Employees may use unsecure services to exchange bank data. ✓ The monitoring of security incidents may be insufficient or non-existent in the current situation. ✓ Data may be exfiltrated or encrypted through malware. ✓ If the device is stolen, locally saved data can be viewed if individual files or the file system are not encrypted. ✓ Further, both employees and management are likely to face increased manipulation efforts to gain access to confidential information.	✓ Employees should be issued with mandatory guidelines informing them of which security solutions they must implement. ✓ Use of simple and standard applications available in Windows (e.g. Windows Defender/Windows Firewall). ✓ Secure endpoints (data retention, secure data transfer, malware protection) and the home-based office itself. ✓ Prohibit third-party access to your information and documents.	RISK	MEDIUM

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
Supply chain risk	Banks rely heavily on a network of interlocking vendors, whether for repetitive tasks (many services providers located in India, Eastern Europe…) or for more high tech services (credit card processing networks, clearing houses…).	✓ Maintaining effective remote operations and oversight of third-party suppliers and providers will be key in order to running business as usual during this period. Service providers could run into problems if their employees get sick or their operations are disrupted. The best execution formula could shift should counterparty settlement be impaired.	✓ Firms should review key service level agreements that are currently in place, with a specific eye on what agreements are flexible and what could go wrong in those that are not. Examine vendors/suppliers operations to determine whether they could be placed under strain. Perform an operational risk assessment internally and with key service providers/suppliers..	RISK	MEDIUM
NEW **Workforce**	On-location activity is particularly important for some industry roles, as with traders who need real-time market access, sales teams that are subject to specific compliance monitoring, or back-office functions who still heavily rely on documents in paper format. This creates a variety of workforce challenges that have been largely untested at scale — until now. Banks will need to focus on different workforce priorities as the COVID-19 crisis unfolds.	✓ In the ST, the priority has been to take control of the situation by addressing workforce wellbeing and engagement, and creating a virtual working environment. ✓ In the MT, as the crisis unfolds, there is a need to stabilise the business by maintaining workforce productivity, understanding skills supply/demand, and carefully planning the de-confinement. *[For more information on this topic, you may watch our webinar titled "From Confinement to De-confinement" available here]* ✓ In the LT, banks will need to embed new ways of working, undertake cost and cash reduction, and plan their workforce strategically.	✓ **We believe that Luxembourg banks should already be planning for the MT**, in particular looking at: • Where employees are required, in what volumes and what work needs to be undertaken as customer demand changes during the de-confinement period; • Re-assess the productivity of virtual working arrangements. ✓ **In the coming 2-3 months banks will have to start thinking about the LT implications**: • Undertake comprehensive workforce planning to determine which people you will need in the new normal (e.g. sales staff at ease in a virtual world); • Consider headcount reduction options where workforce is no longer required; • Redesign roles, work patterns and hours of work to enable flexible working; • Optimise technology infrastructure to ensure productive remote working and digitize processes where possible.	RISK	MEDIUM
NEW **Workplace**	The CSSF expects HBW to last until 25 May. Luxembourg health minister Paulette Lenert and education minister Claude Meisch held a press conference (on 28 April) announcing the country's gradual deconfinement. Companies will have to take social distancing measures applying to their employees and clients in the upcoming months – starting now. These measures will be gradually lifted if the number of new infected cases drops to very low levels as monitored by the Luxembourg COVID-19 Task Force. Furthermore, as HBW may become more and more the norm in the FS industry, the need for extensive office space may be reduced.	✓ In the ST, banks need to start organising the de-confinement, in particular planning actions to ensure compliance with government guidelines, enable social distancing and make the workplace safe. *[For more information on this topic, you may watch our webinar titled "From Confinement to De-confinement" available here]* ✓ In the MT to LT, some banks will have to rethink what real estate do they need (location and design) and how a reduction in office space may impact their financial figures (costs, assets, and liabilities).	✓ **Luxembourg banks should already be planning for de-confinement** by establishing a cleaner and more hygienic work environment (e.g. more stringent, regular daytime cleaning of premises) and ensuring the capacity of the workplace to accommodate staff when social distancing measures are implemented. ✓ **In the LT, banks may consider the following**: • Identify future office space needs under the 'new normal' and compare with current portfolio; • Design workspace to move to "hoteling systems" in services where HBW will become part of the new normal; • Plan for subsequent waves of COVID-19 or other future pandemic/events; • Dispose of excess space, whether owned or leased.	RISK	MEDIUM

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
NEW **AML risk**	Anti-Money Laundering remains a strong focus of regulators. As the EBA highlighted in its 31 March communication on the matter, “experience from past crises suggests that in many cases, illicit finance will continue to flow”. On 10 April, the CSSF released new guidance (in the form of a Circular) on the AML/CFT implications of the COVID-19 pandemic. In its introductory wording the CSSF clearly emphasised that it requires supervised professionals to continue to put in place and maintain effective systems and controls to ensure that Luxembourg financial system is not abused for ML/TF purposes. On 28 April, the Financial Action Task Force (or GAFI) decided to temporarily postpone all remaining evaluations and follow-up deadlines. For Luxembourg, this means that the FATF visit has been postponed to a later date.	✓ Control functions will be put to the test as they quickly review/implement the new CSSF guidelines, often having to work through cross-function teams with IT and business departments. ✓ Banks will have to review the six areas of the financial sector that may be exploited by emerging threats: • Online payment services; • Clients in financial distress; • Mortgages and other forms of collateralised lending; • Credit backed by government guarantees; • Distressed investment products; • Delivery of aid through non-profit organisations.	✓ In the ST, we expect banks to quickly put in place mitigation actions, especially in the areas of particular attention for the CSSF: • AML/CFT business continuity; • Transaction monitoring; • Customer due diligence; • ML/TF risk assessment; • Cooperation with authorities. Regarding customer due diligence, the CSSF refers to the latest FATF Guidance on digital ID to facilitate clients' onboarding purposes. ✓ In the MT, banks will have to: • ensure their processes are flawless for the FATF visit; • put in place the right cross-function teams (mixing compliance, IT and business skills); • consider seeking external help in meeting the challenge.	RISK	HIGH
NEW **Dividend distributions and share buybacks**	On 31 March, The European Banking Authority (EBA) provided more guidelines in reference to its 12 March statement, in which it urged banks to follow prudent dividend and other distribution policies, including variable remuneration, and use capital for ensuring continuous financing to the economy. The EBA remarked that the availability of financial resources generated by the COVID-19 emergency measures should be used to finance the corporate and household sectors and not to increase the distribution of dividends or make share buybacks.	✓ The objective is to ensure Luxembourg banks which committed to support the economy continue to have a robust level of own funds so as to be able to protect policyholders and absorb potential losses.	✓ This measure should be applied by all banking groups at the consolidated level and also regarding significant intra-group dividend distributions or similar transactions, whenever these may materially influence the solvency or liquidity position of the group or of one of the subsidiaries involved. ✓ Contact competent authorities in case of legal requirement to pay-out dividends or make share buybacks. ✓ Ensure that capital distributions within the banking group support the local and the broader European economies.	RISK	LOW

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
NEW **Permanent establishment under BEPS**	On 17 April, the CSSF urged all financial institutions under its prudential supervision to continue favouring working from home. In the coming months, HBW may become the new normal as banks weigh in the benefits for employees (greater flexibility, better work-life balance…) and for their own organization (less employees on site, higher attractivity for new hires, greater productivity…). However, Luxembourg companies employing cross-border staff need to carefully analyse their organizational set up: under the Base Erosion and Profit Shifting (BEPS) project carried out by the OECD, the notion of permanent establishment of dependent agents has been revised.	The new definition of permanent establishment under BEPS has an impact on four areas: ✓ **Personal taxes**: How to count a day worked from home? How is income tax reported and paid? What relief, if any, is there for double taxation? How to report Luxembourg source income in country of residence? ✓ **Social security**: How to count a day worked from home? Where will the individual be subject to social security (25% rule)? How to organize administrative obligations (e.g. A1) ? What are the consequences of moving social security systems (cost benefits administration)? ✓ **Payroll**: Is there a requirement to register a local payroll? Can you adapt the Luxembourg payroll to accommodate exemptions? Are there reporting requirements for non-cash benefits (private medical, accommodation, company car)? ✓ **Corporate tax**: Is there any risk of permanent establishment associated with HBW? Did you assess properly the risk? Did you identify any reporting, compliance or registration obligations in case of permanent establishment?	✓ We expect banking groups will be soon under scrutiny of tax authorities and be subject to Transfer Pricing (TP) documentation requests / tax audits. We recommend our clients to quickly create / review TP documentation and amend those according to the factual situation, i.e. • TP documentation for the group should cover Luxembourg transactions; • TP policy / documentation should be reviewed further to group restructuring; • TP impacts of transfer of functions/assets/risks should be addressed properly (exit tax). ✓ More broadly, we recommend banks to perform a thorough assessment of the implications of implementing HBW. ✓ Banks should consider getting external advice to analyse the potential de facto existence of a permanent establishment in a foreign country; if so we recommend to establish a profit allocation model for the permanent establishment abroad, and validate the profit allocation methodology with the tax authorities.	RISK	HIGH
NEW **DAC6**	On 1 July, DAC6 (EU's 6th Directive on Administrative Co-operation in the field of taxation) will enter into force. The directive requires compulsory reporting of cross-border transactions or arrangements exhibiting so-called "aggressive tax avoidance strategies". However, several countries missed implementing the rules by the 1 January deadline. Practitioners warn that the absence of clear guidance on what should be reported in those jurisdictions may constrain companies to guess or over-report – at the risk of penalties. The current COVID-19 pandemic has added another layer of uncertainty to the DAC6 implementation process. As companies are struggling to keep their heads above water, national authorities, regulators and intermediaries may be distracted by more urgent priorities. It's not inconceivable that authorities might offer some flexibility on DAC6 deadlines.	✓ Because the legislation is retroactive, **all relevant cross-border arrangements established since the directive became law**, between 25 June 2018 and 30 June 2020, **must be reported** by 31 August 2020. ✓ For big holding groups that may have many intercompany transactions that fall within the scope of reportable arrangements, identifying those transactions is a huge task. ✓ Furthermore, the current crisis situation is adding an extra layer of difficulties; performing impact analysis, reviewing files, drafting procedures and implementing controls while collaborators are working from home and not always reachable is certainly a difficult endeavor. The fact that some files may only exist in paper version is also problematic.	✓ We recommend banks to seek external help in meeting the challenge; this will involve, at a minimum, multi-jurisdictional support provided by firms with deep understanding of local requirements, to help intermediaries avoid the risk of penalties. ✓ Additionally, the process will involve the use of proven technology to shoulder what may be a substantial administrative burden.	RISK	MEDIUM

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
UPDATED **Reporting and disclosures**	On 26 March, the Luxembourg Finance Minister extended by 3 months the deadlines for publication of the annual accounts of credit institutions, as well as the related reports (e.g. audit report). The same day, the CSSF decided to grant exceptional delays for the submission of some documents (e.g. ICAAP/ILAAP reports, annual accounts, Long Form Reports …) upon reasoned request to be sent by email to the usual contact person at the CSSF.	✓ These measures offer temporary relief to banks facing operational difficulties related to the current context of Covid-19. ✓ However, it's not too soon to start thinking about early warning disclosures in financial reporting: assets at risk of impairment, disclosures about risk factors and more. ✓ Due to the current situation, the uncertainty and the different possible scenarios may lead to a closer supervision of the supervisor with recurrent and continuous information requirements.	✓ Supervised entities facing a regulatory reporting delay should proactively contact the CSSF through the normal channels and as far in advance from the deadline as possible. ✓ Firms should provide transparency regarding the actual and potential impacts that COVID-19 will have on their operations, financial situation and performance. They should anticipate disclosure in the upcoming reports, in particular if they publish interim accounts.	RELIEF	HIGH
Stress tests	In the context of the COVID-19 outbreak and its global spread since February, the European Banking Authority has decided to postpone the EU-wide stress test to 2021 as a measure to alleviate the immediate operational burden for banks at this challenging juncture. The final timeline for the EU-wide stress test will be communicated in due course.	✓ This measure allows banks to postpone the release of key financial inputs to the regulator, allowing them to pay more attention to the operational issues that are arising and are relevant for the continuity of the bank.	✓ We advise banks to identify resources that were previously planned on the stress test process and that can be reallocated to ensure the continuity of the bank's core operations, including support for customers. ✓ Make use of the flexibility already embedded in existing regulation. ✓ The ECB Banking Supervision's decision to allow banks to cover Pillar 2 requirements with capital instruments other than common equity tier 1 (CET1) is an example.	RELIEF	HIGH
Basel III framework	On 27 March, the Basel Committee announced a series of measures designed to "provide additional operational capacity for banks and supervisors to respond to the impact of Covid-19 on the global banking system". These include pushing back the implementation date of the new Basel III standards, governing bank capital and reporting, by one year to 1 January 2023.	✓ These measures give banks additional time for adopting a new market-risk framework and applying new rules — on capital, accounting and climate risk reporting — thus helping them focus on responding to the various implications of the current crisis.	✓ We advise banks to identify resources that were previously planned on the Basel III program and that can be reallocated to other upcoming regulatory requirements. ✓ Despite the revised timeline, banks should keep an eye on maintaining adequate capital strength in the long term.	RELIEF	HIGH

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
NEW **Guaranteed Loans**	From 18 March 2020 to 31 December 2020, the Luxembourgish government will provide a state guarantee scheme for new bank loans to SMEs and large companies, for up to 6 years. The new credit lines will be guaranteed at 85% by the State and 15% by the participating banks for loans granted during the considered period. On 27 April, the CSSF clarified some aspects of the prudential treatment of loans backed by the Luxembourg State guarantee (law of 18 April 2020). In particular: ▪ in terms of capital requirements regulation (CRR), the guarantee is automatically eligible; ▪ banks are not allowed to use the capital requirement-reducing impact of this measure during the first two months after the concession of the loan; ▪ banks must, once they have formally signed up to the scheme, also consider the concentration risk that they are taking towards Luxembourg; ▪ more time available to collect the money back.	Operational impact: ✓ Increased volume of calls and demand for explanation / information on the implementation of the directive from all kinds of enterprises in Luxembourg. Following CSSF clarifications: ✓ Since the guarantee is automatically eligible, banks do not need to conduct a comprehensive analysis on the capital requirements impacts. ✓ Banks need to provide a concentration risk analysis with regards to Luxembourgish clients.	✓ Determine a plan to manage the increase in requests, by clearly defining responsibilities and relevant authorities to contact in case of doubts. Be prepared for a spike in calls to customer advisors. You may need to redeploy staff, or scale up or down by using contingent workers. Automated systems can help, but your clients may most appreciate human empathy.	RISK	MEDIUM
UPDATED **Branches / ATMs**	The latest CSSF directive requires that home-based working must be privileged over other forms of working, including working from backup centres. Banks have closed their branches or drastically modified access (on appointment only) as Luxembourg went into complete lockdown.	✓ Re-opening of branches will have to strictly follow the government's de-confinement measures. *[For more information on this topic, you may watch our webinar titled "From Confinement to De-confinement" available here]*	✓ Conduct a complete deep-cleaning of all branches, ATMs and locations of client interaction to ensure customers and employees safety. ✓ Consider alternatives to in-person sign-offs (e-signature) and promote solutions that include remote advisory capabilities. ✓ Encourage and support customers to use digital and other virtual channels, wherever possible.	RISK	MEDIUM

KEY RISKS	REGULATORY/ENVIRONMENT CHANGES	IMPACT ON YOUR COMPANY	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
UPDATED **Consumer protection**	Many Luxembourg banks are facing an increase risk of default of their customers. However, consumer protection remains a priority for regulators and has been clearly outlined by the ECB, EBA and CSSF in their latest COVID-19 communications.	✓ Institutions are expected to use a certain degree of judgement and distinguish between borrowers whose credit standing would not be significantly affected by the current situation in the long term, and those who would be unlikely to restore their creditworthiness.	✓ As consumer protection remains the big priority, financial institutions should ensure full disclosure and act in the interest of customers, with no hidden charges or automatic impact on credit ratings.	RISK	HIGH
UPDATED **Phishing and ID theft**	Phishing and identity theft are two of the fastest growing crimes in Europe, and the current situation is making bank customers even more vulnerable.	✓ While firms hardware and software could be vulnerable to potential attacks, misinformation campaigns targeting the clients of specific banks could significantly impact brand reputation.	✓ Firms should proactively reach out to customers in order to preempt any misinformation campaigns. ✓ Further, increased communication could be of benefit to those customers who are seen as higher risk in this regard. ✓ Finally, firms should be highly transparent in their communications with customers to ensure that they are not later accused of hiding particular points.	RISK	HIGH
NEW **Higher customer expectation**	In the context of COVID-19, economic activity is moving online and customers are expecting to digitally access all products and services. Banks need to adjust accordingly, in particular helping retail and small-business customers by expanding the range of services offered online.	✓ Banks should be prepared for a huge increase of digital users. ✓ Older customers who relied exclusively on in-person interaction may be reluctant or unsure how to use digital tools. ✓ Higher importance of customer experience as an element for the acquisition of new clients and the retention of existing ones.	✓ Take advantage of the customer experience trends of the latest years and turn them into competitive advantages. ✓ Support the majority of the customer base in the transition to online banking (call centres and live chats). ✓ Introduce new experiences for customers in difficult financial conditions and provide reassurance about investments and savings.	RISK	MEDIUM

Key PwC resources

"From Confinement to De-confinement" webinar

It is now time for every public and private organisation to prepare their exit strategies and return to a “new normal”. The process, novel to most of us, requires to think through operations, infrastructure, human resources, security aspects, among others.

We organised a webinar session, animated by Anne-Sophie Preud'Homme (COO, PwC Luxembourg), François Mousel (Market leader, PwC Luxembourg) and Roy Coppieters (Crisis management leader, PwC Belgium) to answer your questions.

Watch the recording here.

Covid-19 Free Hotline

PwC Luxembourg is launching a hotline to help local businesses face and navigate the current disruption. As a responsible corporate citizen, our firm will assist you benevolently to understand and apply the measures taken by the Luxembourg government in relation to the Covid-19 outbreak, which might impact your business and people.

Don’t hesitate to get in touch at +352 49 48 48 5959.

E-signature - Setting up a secured electronic signature in 48 hours

In the context of home-based working, a secured electronic signature process has become the standard for decision makers to validate bank transfers, contract signatures, purchase orders, etc.

Thanks to the expertise gained in both audit signature, and the rapid implementation of e-signature solutions for international groups in several countries, PwC is in a position to assist you in the deployment of a highly-secured solution in 48 hours.

Learn more here.

Key PwC tools

Perform plus productivity suite

Perform Plus is our methodology and toolset focused on improving employee productivity. The suite comprises a series of tools that allow teams to virtually conduct huddles, scrums, and set/measure specific goals (e.g. project goal accomplishment, operational production levels, error rates, etc.). This helps better connect teams and maintained and even improved productivity, providing managers with the ability to systemically keep track of things like employee morale. Here is a brief video which describes Perform Plus and how it is used as well as an attached presentation.

Productivity hub

Productivity Hub is a tool to better understand and measure the nature of work at the employee level. It involves breaking down an individual's key tasks and then time tracking against either tasks or deliverables. With this data, the tool allows you to create a series of dashboards that compare the performance of individuals and teams. We have used the tool on groups of up to 500 people in 13 countries and have found that it boosts productivity, on average, at least 20-25%. Please see the link for a brief video on Productivity Hub here.

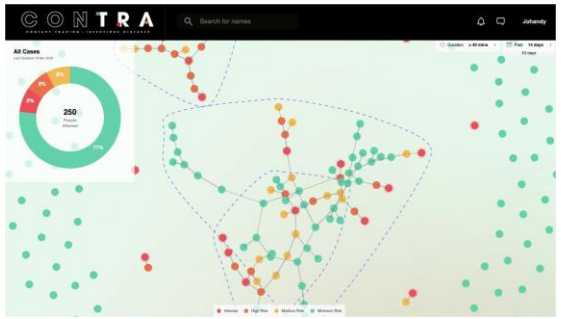
Digital fitness app

The DFA is an app to help provide additional digital training/learning for the workforce. It includes a baseline assessment (a digital fitness score) and a series of training modules to improve skills and capabilities of individuals, allowing them to boost their capabilities and associated scores. It is being used by a number of clients during the crisis to accelerate existing training activities and equip their teams with the skills needed to digitise their businesses and so enhance productivity. Here is a video on DFA.

Key PwC tools

Contra: Contact Tracing and Tracking

Contra is a simple, but effective solution for Covid-19 contact tracing, that swaps a digital signature with anyone it's in close contact with – and in turn, who that person has been in contact with too. The platform aggregates relevant data and produces a visual network of people who have been in proximity with each other, grouped by location and time of contact. If a suspected case occurs, we can then immediately understand the people at risk, and take action. See here for an overview of the Contra tool.

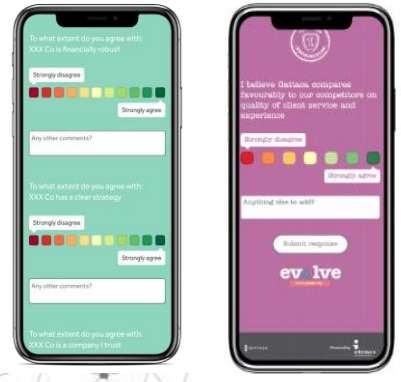


Workforce Disruption Analytics

PwC's Business Continuity Solution uses your data to provide a coherent overview of at-risk roles and where skills are best matched.
By combining client input from a Business Function Criticality Assessment with HCM data, we can visualise capability of operations across the business. We couple this with a skills-matching algorithm that uses employee skills data to identify the best-placed redeployment of talent to minimise any operational and financial shortcomings post-crisis. Please see here for an overview of PwCs Workforce Disruption Analytics.

Intrinsicx

Intrinsicx is a unique, real-time technology application that helps organisations to monitor and proactively manage productivity, sentiment, behaviour, culture and engagement, across employee and other key stakeholder communities. It provides organisations with deep and continuous insights allowing them to track progress against desired outcomes and drive tangible actions. Here is an overview of what Intrinsicx can do.



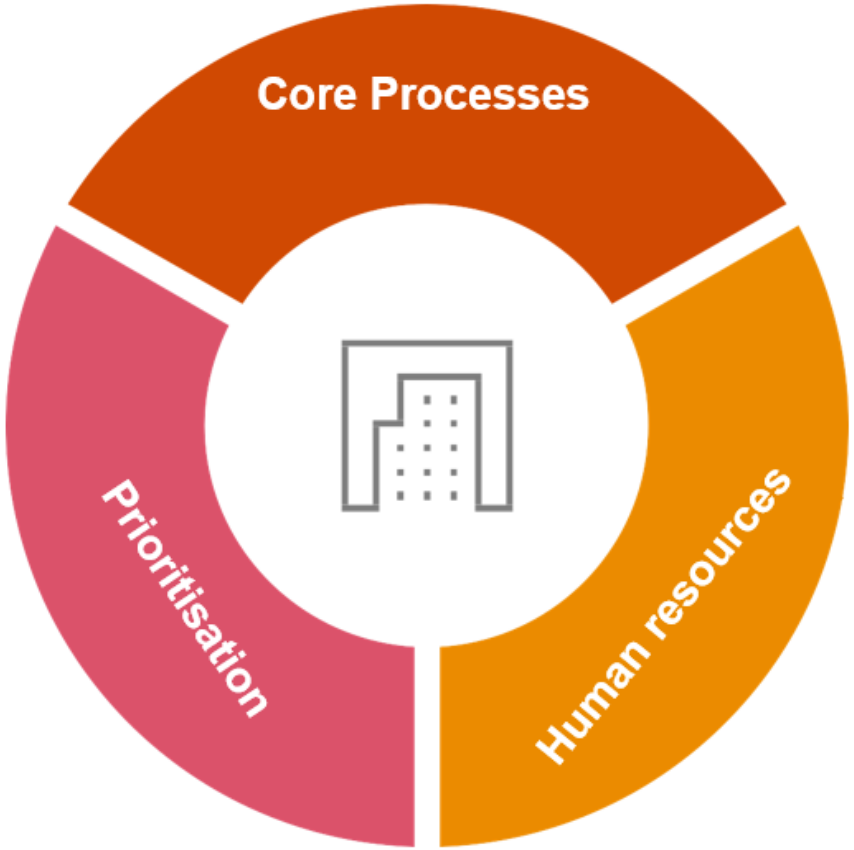
Working together securely during the COVID-19 crisis

A manual by **PwC Cyber Security & Privacy**

Banking
May 2020

pwc

Which processes are essential for the Business Continuity?



Core processes

Which business departments and processes require ad hoc (and appropriate) solutions?

Which processes provide essential services for the company and/or its clients?

Human resources

Which employees or user access rights are essential for maintaining these processes?

Prioritisation

Which departments and processes will be prioritised for co-working?

Should important IT services be prioritised to ease the burden on them, at the expense of non-essential services and user access rights?

Threats when working from home

Endpoint protection is the key security consideration in remote working

Data exchange over unsecure channels

Users use unsecure services to exchange company data.

Insufficient malware protection

No – or insufficient – malware protection is installed. Users have administrator rights.

Data may be exfiltrated or encrypted through malware.

Data visible to third parties

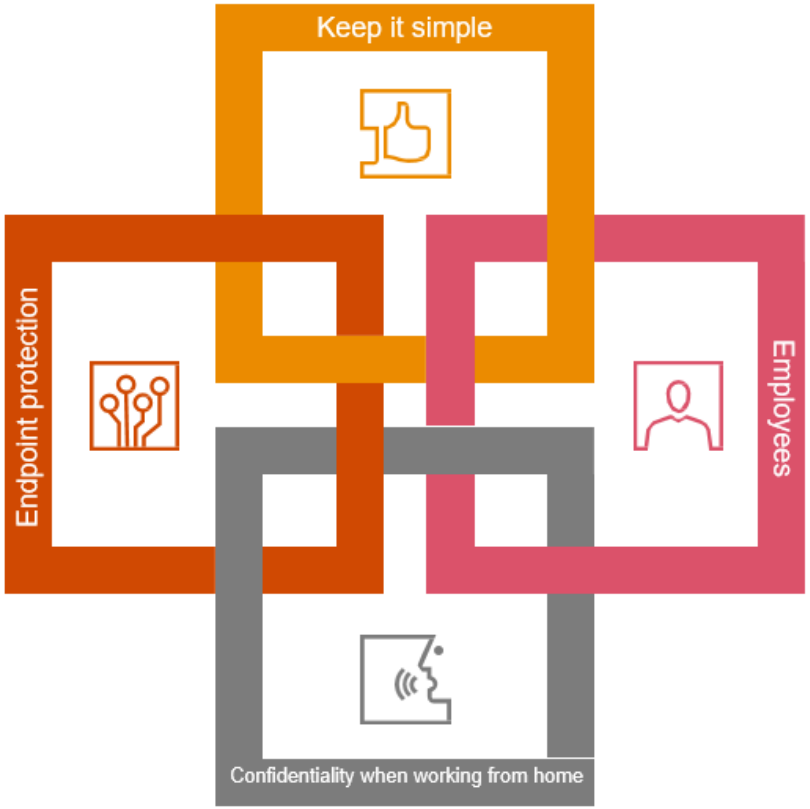
Company data may be visible to third parties looking at the physical device if the room layout or access protection is insufficient.

Unencrypted data storage devices

If the device is stolen, locally saved data can be viewed if individual files or the file system are not encrypted.

IT security for remote working

How to make your IT more secure when working from home



Employees

Employees should be issued with mandatory guidelines informing them of which security solutions they must implement.

Keep it simple

Standard applications that are available in Windows, such as Windows Defender and Windows Firewall, should be used to keep the support workload low.

Endpoint protection

Securing endpoints (data retention, secure data transfer, malware protection) and the home-based office itself are the key priorities for remote working.

Confidentiality when working from home

Keeping confidential information confidential is particularly important when working from home (e.g. during telephone calls and meetings). Third parties must not be allowed to catch sight of information and documents.

Is co-working possible?

YES

Development and use

What you must pay attention to:

- System resources
- Restrictions
- Licences
- Informing employees
- Compliance with regulations
- Security risks caused by system demand

NO

Selection and implementation

What you must pay attention to:

- Choosing the right products/solutions
- Appropriate scaling
- Licences and contract durations
- Implementation effort
- Informing employees
- Security aspects and risks
- Potential removal of the solution

Co-working IS POSSIBLE.

What you must pay attention to:

- System resources
- Restrictions
- Licences
- Informing employees
- Compliance with regulations
- Security risks caused by system demand

Upscaling

of current remote working options.

Implementation

Are there enough system resources (WAN, LAN, CPU, RAM) for all the employees who need them?
Where are the bottlenecks in the solution?
Does system demand pose a security risk?

Licences

Where are licences required?
Are there enough licences?
Who needs licences?
Are new licences required?
Who acquires the licences?

Monitoring

How are user requirements managed?
How are the solutions monitored?

Regulations

Are the existing regulations (e.g. on company information) being adhered to?
Do guidelines need to be adapted?

Risks

What are the risks?
How can risks be prevented?

Employees

How are the employees informed of the possibilities for co-working?
What information do the employees need (handout, instruction manual)?

Planning

What are the requirements? Which products are concerned?

System resources

On-premises vs on the cloud
How quickly can the solution be made available?
Can the solution be rolled out remotely?

Licences

Commercial vs open source
Where are licences required?
Are there enough licences?
Who needs licences?
Are new licences required?
Who acquires the licences?

Monitoring

How are user requirements managed?
How are the solutions monitored?

Regulations

Are the existing regulations (e.g. on company information) being adhered to?

Do guidelines need to be adapted?

Risks

What are the risks?

How can risks be prevented?

Employees

How are the employees informed of the possibilities for co-working?

What information do the employees need (handout, instruction manual)?

Co-working IS NOT POSSIBLE.

What you must pay attention to:

- Choosing the right product
- Appropriate scaling
- Licences and contract durations
- Implementation effort
- Informing employees
- Security aspects and risks
- Potential removal of the solution

Possible collaboration solutions – Voice and video

Solution	Security	Risk			Implementation			
	Security aspects / Best practice	Low	Medium	High	Licensing	Deployment	Standards	Website
Mobile phone	Communication is unencrypted			×	Not required	Already exists	Open	-
Microsoft Skype for Business	P2P communication, encrypted, MFA	×			$2 per user per month; comes for free with Office 365	Installation, fast	Proprietary	skype.com
Google Hangouts Meet/Chat	Transport encryption only, MFA		×		From €4.68 per month; licensing through G Suite	Browser, fast	WebRTC	hangouts.google.com
Cisco Webex	End-to-end encryption, MFA	×			From €12.85 per month per host	Browser, installation	WebRTC/proprietary	webex.com
Zoom	Transport encryption, end-to-end encryption (optional)	×			Free for short meetings with few participants	Installation	Proprietary	zoom.us
Slack	Transport encryption only, MFA		×		From €6.25 for teams of up to 15 members	Installation	WebRTC	slack.com
Microsoft Teams	Transport encryption only, MFA		×		From €4.20 per month per user for Office 365	Browser, installation	Proprietary	products.office.com/de-DE/microsoft-teams
Jitsi	End-to-end encryption, self-hosted	×			Open source	Server installation	Open	www.jitsi.org

Commercial use of the solutions listed in this section usually entails licence costs. When selecting a solution, you should always check which versions can be used for business purposes. As some solutions and services are not GDPR-compliant, you should moreover check whether personal data is processed when the solution/service is used. The data-protection information outlined here is provided by the manufacturers, and has not been explicitly checked by PwC.

Possible collaboration solutions – Data exchange

Solution	Security	Risk			Implementation			
	Security aspects / Best practice	Low	Medium	High	Licensing	Deployment	Risks	Partner
Email (on-premises) (end users/technical staff)	• Mailbox can be accessed externally over the Internet • Encrypted data transmission (end-to-end possible) • Multi-factor authentication	×			Additional licences not usually required	Fast	• Attacks from outside • Insufficient resources	OWA
Email (cloud) (end users/technical staff)	• Cloud applications are linked to central directory services • Cloud providers based in Germany • Multi-factor authentication		×		Licences must be acquired	Very fast	• Loss of data sovereignty • Potentially no data protection	Office 365
Applications/file storage (on-premises) (end users/technical staff)	• File storage can be accessed externally over the Internet • Multi-factor authentication		×		Additional licences may be required	Medium	• Attacks from outside • Insufficient resources • Unsecure transmission/ storage of sensitive files	SharePoint, Nextcloud, ownCloud, Jira, Confluence
Applications/file storage (cloud) (end users/ technical staff)	• Cloud applications are linked to central directory services • Cloud providers based in Germany • Multi-factor authentication		×		Licences must be acquired	Very fast	• Loss of data sovereignty • Potentially no data protection • Unsecure transmission/ storage of sensitive files	Office 365, G Suite, Mega, Jira, Confluence, LibreOffice Online
Instant messaging (end users)	• Data is packaged and password-protected before being sent • Separation of professional and personal files			×	Additional licences not usually required	Very fast	• Data transfer and storage may be unencrypted at operator level	Threema, WhatsApp, Slack
Analogue data exchange (end users)	• Data saved onto encrypted and secure USB sticks • Secure transportation		×		Not required	Fast	• Flows of company data • Loss of data storage devices	BitLocker, VeraCrypt

Commercial use of the solutions listed in this section usually entails licence costs. When selecting a solution, you should always check which versions can be used for business purposes. As some solutions and services are not GDPR-compliant, you should moreover check whether personal data is processed when the solution/service is used. The data-protection information outlined here is provided by the manufacturers, and has not been explicitly checked by PwC.

Possible connectivity solutions – Connecting remote workplaces

Solution	Security	Risk			Implementation			
	Security aspects / Best practice	Low	Medium	High	Licensing	Deployment	Risks	Partner/Solutions
VPN (end users/technical staff)	Use of a secure key and up-to-date cryptographic algorithms; multi-factor authentication; no split tunnelling; load balancing	×			Depends on the solution – sometimes expensive/ complex	Medium	Heavy load on VPN gateway/WAN	Always On VPN, IPsec (almost every firewall)
VDI on-premises (end users/technical staff)	Securing the infrastructure; appropriate load balancing; dimensioning; multi-factor authentication	×			Time-consuming	Slow	Configuration errors, complex, scaling	Citrix, VMWare Horizon, Nutanix, NVIDIA VDI
Cloud VDI (end users/technical staff)	Securing the cloud environment; multi-factor authentication; taking data protection into consideration		×		Flexible, fast	Fast	Data protection not guaranteed, data sovereignty	Amazon WorkSpaces, itopia, Azure VDI
Terminal server (end users/technical staff)	Securing the connection (VPN)		×		Flexible, fast	Medium	Scaling	Microsoft terminal server
Remote desktop (technical staff)	Limiting access at user and machine level; data protection			×	Flexible, medium to fast depending on solution	Very fast	Potentially unsecure connection, poor scaling	TeamViewer, Microsoft Remote Desktop, Splashtop
SSH (technical staff)	Use of secure keys/SSH over VNP; security for technical users; secure configuration of the SSH server	×			Not required	Very fast	Unsecured users	PuTTY, Bitvise, OpenSSH
Local working (end users)	Securing the endpoints (encryption); regular data backup; secure data exchange	×			Not required	Fast	Loss of data, inconsistent data sets	Use of workstation at home

Commercial use of the solutions listed in this section usually entails licence costs. When selecting a solution, you should always check which versions can be used for business purposes. As some solutions and services are not GDPR-compliant, you should moreover check whether personal data is processed when the solution/service is used. The data-protection information outlined here is provided by the manufacturers, and has not been explicitly checked by PwC.

Possible endpoint solutions – Preparing the hardware for remote working

Solution	Security	Risk			Implementation			
	Security aspects / Best practice	Low	Med.	High	Licensing	Deployment	Risks	Partner/Solutions
Corporate mobile device (end users/technical staff)	Securing the endpoints (encryption); regular data backup; secure data exchange; regular security updates; endpoint security	×			Flexible, fast	Medium	Poor scaling for acquisition and deployment	Dell, HP, Lenovo, Apple, Fujitsu
Corporate workstation (end users/technical staff)	Securing the endpoints (encryption); regular data backup; secure data exchange; regular security updates; endpoint security	×			Flexible, fast	Medium	Poor scaling for acquisition and deployment	Dell, HP, Lenovo, Apple, Fujitsu
BYOD/UYOD (end users)	Exclusively over VDI where possible*		(×*)	×	Flexible, fast	Very fast	Data protection not guaranteed; data sovereignty; insufficiently secure endpoints	Chromebook, Samsung, Apple, Huawei, etc.
Chromebook / iPad / tablet / smartphone (end users)	Securing the OS; up-to-date firmware; mobile device management; endpoint security			×	Flexible, fast	Medium	Complex to secure	Microsoft terminal server

Commercial use of the solutions listed in this section usually entails licence costs. When selecting a solution, you should always check which versions can be used for business purposes. As some solutions and services are not GDPR-compliant, you should moreover check whether personal data is processed when the solution/service is used. The data-protection information outlined here is provided by the manufacturers, and has not been explicitly checked by PwC.

Your PwC Covid-19 response team available for your support

Banking Industry Leader
Roxane Haas
roxane.haas@pwc.com
+352 49 48 48 2451

Financial Services Industry Leader
Olivier Carré
olivier.carre@pwc.com
+352 49 48 48 4174

Advisory Leader
François Génaux
francois.genaux@pwc.com
+352 49 48 48 4175

Banking Risk Leader
Jean-Philippe Maes
jean-philippe.maes@pwc.com
+352 49 48 48 2874

Banking Tax Leader
Murielle Filipucci
murielle.filipucci@pwc.com
+352 49 48 48 3118

Banking Technology Leader
Patrice Witz
patrice.witz@pwc.com
+352 49 48 48 3533

Cyber Security Leader
Koen Maris
maris.koen@pwc.com
+352 49 48 48 2096

Crisis Management and Resilience
Thomas Wittische
thomas.wittische@pwc.com
+352 49 48 48 4181

Banking Outsourcing Leader
Florian Bewig
florian.bewig@pwc.com
+352 49 48 48 4169

You can also visit our dedicated Covid-19 website under: www.pwc.lu/covid-19

Explanatory notes

Management attention dashboard explanation

- We have developed a dashboard to support you in determining where within your organisation you need to focus attention given the volatile environment caused by COVID-19

- We define four main areas of attention namely: Balance Sheet, Operations, Regulatory and Compliance as well as Client Impact. Although regulatory changes and risks are drivers there are some impacts such as regulatory and risk reporting that will demand attention.

- The temperature of each of these four areas shown by the thermometer demonstrates the attention required and will change overtime

- This is based on various triggers of regulation, risk and operations which are being set off due to current circumstances. This is shown and broken down in the various relevant factors in the speedometers below the thermometers.

- For further detail of the factors you can get an initial explanation of the impact and key actions from slide 7 to 14. For further information you can contact us through email or phone at anytime. The contact details of relevant persons are on slide 29.

Explanatory notes

Market dashboard explanation

- **Corporate high-yield bond spreads** measure the gap between the yield of low-grade bonds and that of stable high-grade bonds of similar maturity. A spike in the spread signals low market's risk tolerance, increased perceived risk of junk bonds' default, as well as higher risk premia demanded by investors.

- **10-years government bonds yield spreads**: Low ten-year government bonds yield capture investors' tendency to divest towards longer term bonds once they expect a slowdown in real economic activity and in inflation in the short-term. If the impact of a foreseen recession is expected to be asymmetric among countries, bonds from riskier countries are likely to rise more compared to those from countries whose debt-to-GDP ratio is considered to be more sustainable.

- **VIX and Volatility Indexes**: As a consequence of sharp stock price declines, we usually observe high volatility in the markets. Commonly known as the "Fear Index", the role of VIX is to reflect increasing or decreasing market volatility by using option contracts on the S&P 500. Given that stock market downturns are a leading indicator for economic slowdowns (because companies are expected to have less revenues, thus investors sell them), rising volatility (which is usually a product of declining stock markets) could be an important indication that a recession is close.

- **Sovereign CDS**: By definition, a Contract Default Swap (CDS) offers protection to its buyer in case the bond that the contract is based on defaults. In other words, the owner of a CDS will receive an amount of money if the underlying bond defaults. If the price of such contracts increases for a specific sovereign bond, this means that the probability of that particular bond defaulting is higher. Therefore, by looking at CDS contracts for sovereign bonds we can form an opinion on whether a country will face issues servicing its debts (high CDS price) or if there is no such risk (low CDS price).

- **The Corporate CDS Spread:** Same principle as Sovereign CDS but applied to a corporate instead of a country. The higher the CDS spread, the higher the probability of a particular corporate to default.