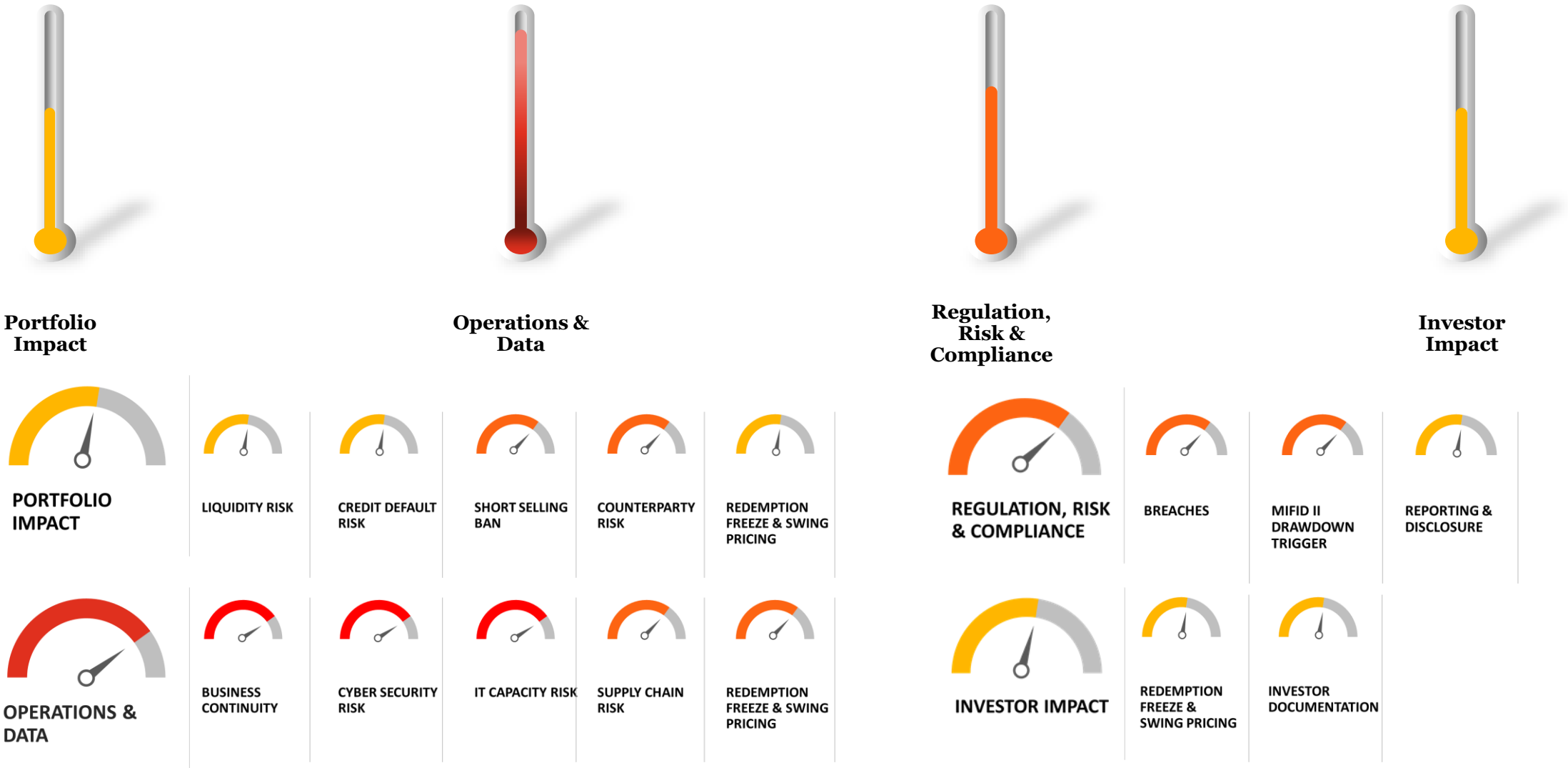
COVID-19 Business Briefing

Updated Edition

Asset & Wealth Management
May 2020

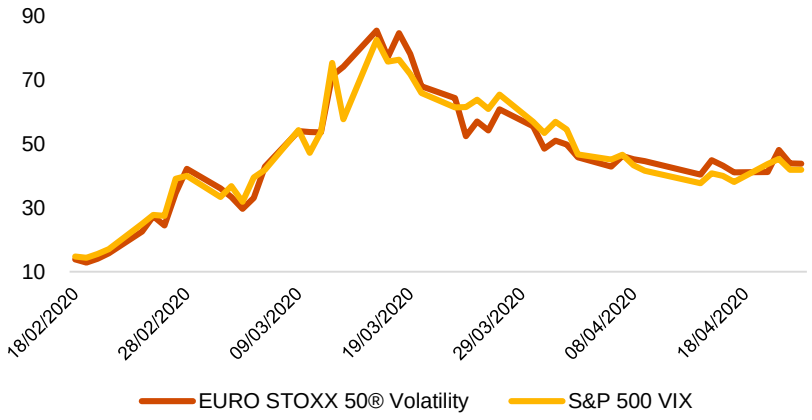
pwc

Management attention dashboard

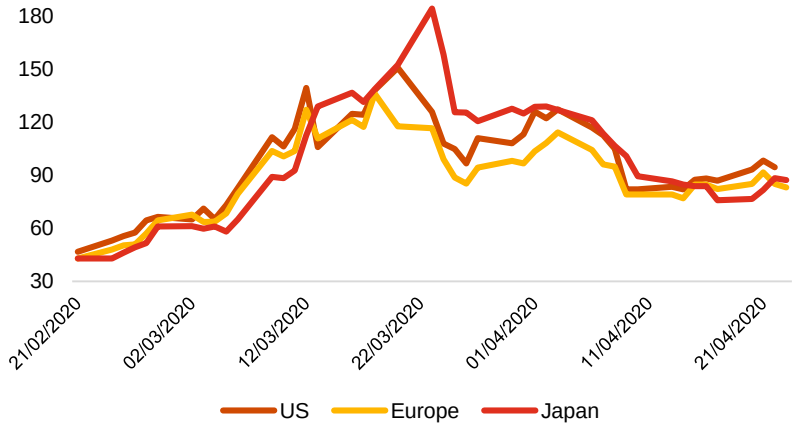


Market dashboard

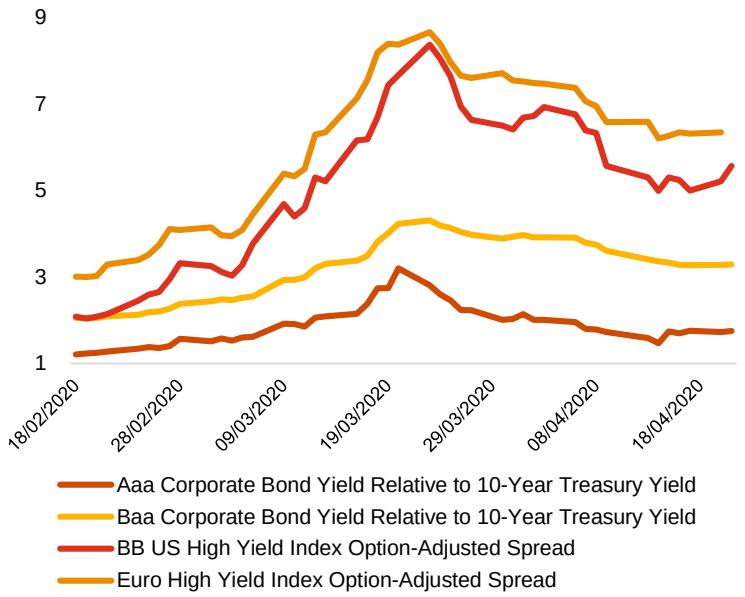
Equity market volatility indices



Corporate CDS spread / 5Y Investment grade



Euro and US Corporate bond yield spread in %



10-year government bond yield spread across selected economies as of April 23

Country	Yield	Vs Bund	Vs T-Note	1w Variation
Austria	0.093	50	-53.1	10.7%
Belgium	0.221	62.8	-40.3	10.2%
Canada	0.615	102.2	-0.9	-3.1%
France	0.118	52.8	-50.3	7.3%
Germany	-0.407	0	-103.1	6.6%
Italy	2.042	244.9	141.8	8.7%
Japan	-0.002	40.3	-62.6	-2.4%
Netherlands	-0.105	30.2	-72.9	6.8%
Spain	1.055	146.3	43.2	20.0%
Switzerland	-0.392	1.6	-101.5	4.0%
United Kingdom	0.327	73.4	-29.7	2.1%
United States	0.624	103.1	0	-4.2%

Sovereign CDS 1-month change as of April 23

Country	S&P Rating	5Y CDS	1m variation	Default Probability
Norway	AAA	17.0	-2%	0.3%
Denmark	AAA	17.9	0%	0.3%
Sweden	AAA	18.1	-4%	0.3%
Netherlands	AAA	19.5	-3%	0.3%
USA	AA+	19.8	-15%	0.3%
Singapore	AAA	20.2	-22%	0.3%
Finland	AA+	21.9	4%	0.4%
Austria	AA+	22.7	0%	0.4%
Germany	AAA	25.5	13%	0.4%
New Zealand	AA	30.5	-38%	0.5%
Canada	AAA	33.0	0%	0.6%
Japan	A+	35.2	-23%	0.6%
South Korea	AA	36.9	-35%	0.6%
Ukraine	AA	38.7	-14%	0.7%
Hong Kong	AA+	41.0	4%	0.7%
France	AA	44.4	3%	0.7%
Belgium	AA	44.5	9%	0.7%
Ireland	AA-	46.8	-4%	0.8%
Slovakia	A+	51.2	-2%	0.9%
China	A+	51.6	-29%	0.9%
Poland	A-	62.8	5%	1.1%
Qatar	AA-	65.0	0%	1.1%
Croatia	BBB-	75.3	-14%	1.3%
Israel	AA-	76.6	11%	1.3%
Philippines	BBB+	90.5	-44%	1.5%
Chile	A+	114.0	-30%	1.9%
Malaysia	A-	116.5	-37%	1.9%
Portugal	BBB	136.3	14%	2.3%
Spain	A	139.2	12%	2.3%
Russia	BBB-	179.1	-36%	3.0%
India	BBB-	197.5	-13%	3.3%
Indonesia	BBB	221.4	-24%	3.7%
Colombia	BBB-	248.1	-26%	4.1%
Bahrain	B+	255.0	0%	4.3%
Italy	BBB	265.3	44%	4.4%
Mexico	BBB	272.8	-3%	4.6%
Greece	BB-	281.6	28%	4.7%
Brazil	BB-	313.4	-6%	5.2%
South Africa	BB	420.5	3%	7.0%
Pakistan	B-	596.5	-14%	9.9%
Turkey	B+	604.3	4%	10.1%
Egypt	B	626.1	-4%	10.4%
Ukraine	B	626.2	-36%	10.4%
Argentina	SD	9169.6	-31%	100.0%

KEY RISKS	REGULATORY CHANGES	BUSINESS IMPACTS	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
Reporting and disclosure	✓ On 14 April, the CSSF confirmed that it intends to comply with ESMA public statements regarding deadlines applicable under the UCITS Directive and under the AIFMD for annual and half-yearly reports. ✓ On 16 April 2020, the CSSF confirmed that deadlines for the reports to be submitted by UCIs, SIFs, SICARs, investment fund managers, pension funds and securitisation undertakings could be extended under certain conditions. NEW	✓ Investment fund managers who anticipate that annual and half-yearly reports will be published beyond the regulatory deadlines must inform the CSSF promptly thereof, only by email, with an indication of the reasons for the delay and, to the extent possible, the estimated date of publication. ✓ Investment fund managers must also inform investors as soon as possible of this delay, the reasons for such a delay and, to the extent possible, the estimated date of publication. NEW	✓ Assess **reporting inputs** status AND related parties and delegates inputs ✓ Assess **state of reporting finalisation** compared to deadline ✓ Define **CSSF communication plan** in case of 'justified' reporting delay ✓ Provide for **Conducting Officer** committee decision ✓ Provide for **Board of Directors** acknowledgement / decision	RELIEF	MEDIUM
Breaches & CSSF Notifications	✓ On 16 April, the CSSF confirmed that it does not require passive investment breaches (i.e. a breach beyond the control of the fund) to be notified (limit of article 42(3) of the 2010 Law). ✓ Breaches of the VaR limit as defined by the UCITS Directive can also be considered as passive breaches. ✓ Upon occurrence of a passive breach, any additional risk exposure taken by the fund increasing the overall level of risk of the portfolio (i.e. VaR usage increasing) should be viewed as an active investment breach. NEW	✓ The passive breach should however not preclude The UCITS from continuing to manage the fund. If a new position does not increase the level of risk of the fund, it should not be viewed as an active breach. ✓ The CSSF expects investment fund managers to take appropriate steps to meet the limit within a reasonable time period, thereby taking account of the prevailing market conditions and of the best interests of investors. ✓ In case of an active breach of the VaR limit, the notification to the CSSF should include a minimum set of information: http://www.cssf.lu/en/supervision/ivm/ucits/forms/ NEW	✓ Portfolio management/Conducting Officers to monitor **portfolio diversification and investment policy rules** when (fire) selling securities ✓ Prepare **identification and notification procedure for large redemptions** (10% NAV per day / 30% NAV per week) ✓ Prepare **identification and notification procedure for VAR limit breaches** ✓ **Update Prospectus** in case required and 'abnormal market situations' clause not included	RISK	HIGH

KEY RISKS	REGULATORY CHANGES	BUSINESS IMPACTS	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
NAV suspension, Gating & Swing Pricing	✓ On 7 April 2020 the CSSF confirmed that UCIs can increase the applied swing factor beyond the maximum swing factor laid down in the fund prospectus in the following situations: ✓ If the fund prospectus formally offers the possibility (Case 1), the Board of Directors of the UCI or, if applicable, the Management Company can decide to increase the swing factor in accordance with the provisions and conditions of the prospectus. ✓ If the fund prospectus does not offer the possibility (Case 2), the CSSF permits, on a temporary basis, the Board of Directors of the UCI or, if applicable, the Management Company, given the current exceptional market circumstances involved by the COVID-19, to increase the swing factor beyond the maximum level mentioned in the UCI prospectus. ✓ In both cases, the decision must be duly justified and take into account the best interest of the investors. NEW	✓ The UCI has to provide the CSSF with a detailed notification of the resolution, including a specific explanation as to why it was taken. ✓ The Board of Directors must communicate this decision to current, as well as new, investors through the usual communication channels as laid down in the prospectus. ✓ For the second case, the communication to investors has to be made before applying an increase of the swing factor beyond the maximum swing factor laid down in the fund prospectus. The CSSF must simultaneously receive a copy of this communication to investors. ✓ Furthermore, for the second case, an update of the UCI prospectus to formally provide for the possibility to the Board of Directors of the UCI or, if applicable, the Management Company to go beyond the maximum level under certain predefined conditions, has to be performed at the earliest convenience. NEW	✓ The **revised swing factors have to be the result of a robust internal governance process** and are based on a robust methodology (including market / transaction data-based analysis) that provides for an accurate NAV which is representative of prevailing market conditions. ✓ An **appropriate communication to investors has to be put in place through the usual communication channels**. When the fund prospectus does not yet offer the possibility to go beyond the maximum level laid down in the fund prospectus, this communication must be made before applying the increased swing factor beyond the maximum level laid down in the fund prospectus. ✓ For a swing factor adjustment going beyond the maximum swing factor laid down in the UCI prospectus in force, it is **important to document the rationale behind the decision** in order to anticipate a potential justification request from the CSSF**.** NEW	RELIEF	HIGH
Business continuity	✓ Further to the confirmation by the Luxembourg government, on 15 April 2020, that the lockdown will be extended with limited exceptions until at least 25 May, the CSSF urges all financial institutions under its prudential supervision to continue favoring working from home. As already mentioned in the CSSF communications of 2 March and 17 March, satisfactory IT security conditions should be guaranteed and no prior authorisation is needed for such work arrangements. UPDATE	✓ The majority of investment fund managers should have business continuity plans already. However, many of these plans are not able to handle a fast moving situation such as COVID-19. ✓ 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.	✓ Firms should address their **crisis communications** and be transparent with decisions that are being made ✓ Firms should identify the **key decision points** that must be taken and decision governance (frequency & decision makers) ✓ Consider re-assessing the **enterprise wide risk framework** to be better able to address any new risks ✓ Identify and address risks at **sub-delegates and related parties** to the value chain (e.g. offshore providers shut-down)	RISK	HIGH
Supply chain risk	✓ In Poland and India (the main financial offshore centers), nationwide lockdowns were announced on March 24 and are now extended for an undefined period of time in Poland and May 3 in India. ✓ AWMs rely heavily on a network of interlocking vendors, and this has increased with the advent of FinTech. In fact, virtually every aspect of modern markets now depends on the availability of third parties, such as clearing houses, depositories, data vendors, etc. which could also be located offshore, hence increasing the risk. UPDATE	✓ Uncertainties remain with regards to lockdown periods that might be extended ✓ 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.	✓ **Review key service level agreements** that are currently in place, with a specific eye on what agreements are flexible and the level of BCP ✓ Examine **vendors/suppliers operations** across technology, compensation, accounting, etc., to determine whether they could be placed under strain ✓ Perform an **update on the operational risk assessment** internally and with key service providers/suppliers to ensure all understand the possible areas of disruption	RISK	HIGH

KEY RISKS	REGULATORY CHANGES	BUSINESS IMPACTS	KEY ACTIONS TO TAKE	RISK or RELIEF	IMPACT LEVEL
Cyber risk, HBW Policy & access rights management	✓ Further to the confirmation by the Luxembourg government, on 15 April 2020, that the lockdown will be extended with limited exceptions until at least 25 May, the CSSF urges all financial institutions under its prudential supervision to continue favouring working from home. ✓ In Luxembourg, the government has, by way of decree, permitted digital meetings, under certain conditions. ✓ Further, the CSSF has given guidance to the risks related to cyber security. ✓ On 10 April, the CSSF released the circular 20/740 to provide guidance to all professionals subject to anti-money laundering and counter-terrorism financing (AML/CFT) in relation to the money laundering and terrorism financing (ML/TF) risks and AML/CFT implications of the COVID-19 pandemic ✓ . NEW	**Threats stemming from Home-based Working (HBW)** ✓ Users use unsecure services to exchange company data ✓ Your data may be visible to third parties looking at the physical device if the room layout or access protection is insufficient ✓ 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 NEW	✓ Review **Home Based Working policy** to include remote access rules, cyber security standards and taxation principles ✓ **Approved list of standard applications** ✓ **Secure endpoints** (data retention, secure data transfer, malware protection) and the home-based office ✓ Review **access rights policy and management procedure** to avoid unauthorized third-party access to your information and documents NEW	RISK	HIGH
IT capacity risk	✓ The CSSF, on 22 March, called for an immediate review of current organisational setups by supervised entities. Specifically putting forth that firms should 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."	✓ Asset Managers' infrastructure is not usually designed for all employees to connect the company network remotely and a solution enabling employees to continue their work must be put in place as quickly as possible. ✓ Managers' infrastructure has not been tested for security loopholes, and thus gives rise to risks for data protection and data security that should not be underestimated. ✓ Shifted priorities within the IT organisation may lead to the monitoring of security incidents being insufficient or non-existent. ✓ Higher focus on service deployment, rather than on functional and security tests prior to implementation. NEW	**Defining Priorities** ✓ **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? ✓ **Prioritization:** Which departments and processes will be prioritized? Should important IT services be prioritized to ease the burden on them at the expense of non-essential services and user access rights? **If HBW is possible**, you must pay attention to system resources, restrictions, licenses and informing employees, compliance with regulations and security risks caused by system demand. NEW	RISK	MEDIUM

Working together securely during the COVID-19 crisis

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

Asset & Wealth Management
May 2020

pwc

Challenges

Pandemic

Faced with the current threat of COVID-19, many companies are having to connect their employees remotely.

Security

Unlike established structures, ad hoc ones built for this situation have not been tested for security loopholes, and thus give rise to risks for data protection and data security that should not be underestimated.

Infrastructure

Companies' infrastructure is not usually designed for all employees to connect the company network remotely.

A solution enabling employees to continue their work must be put in place as quickly as possible.

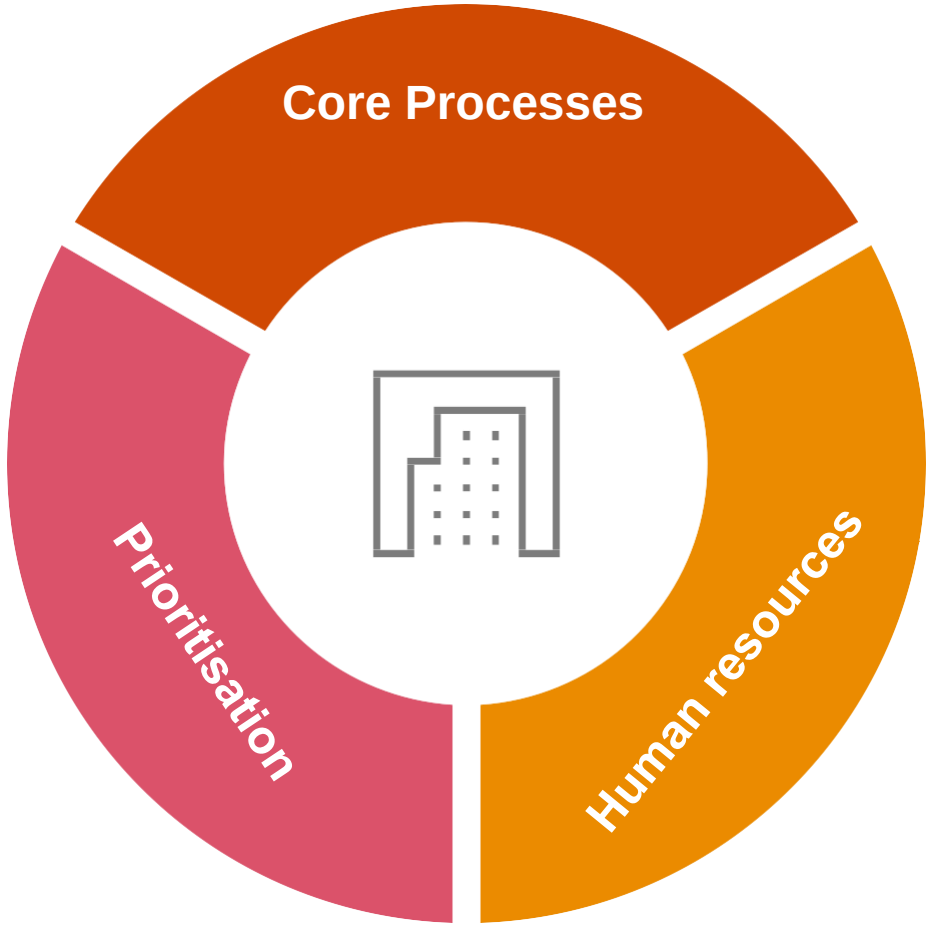
Solution

The aim of this manual is to help you find the right co-working solution for your business.

1

Risks, priorities and compliance

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?

Compliance

Ensuring that problem-solving approaches conform to the organisation's **security regulations**.

Adhering to applicable laws (e.g. on **data protection**) and contractual provisions on cybersecurity (e.g. client contracts).

Taking **security standards** into consideration when procuring solutions for emergency operations.

The risks of providing ad hoc solutions

IT usage

Potentially very heavy load on IT services, IT infrastructure and bandwidth due to increased remote access to the company network.

Monitoring

Shifted priorities within the IT organisation may lead to the monitoring of security incidents being insufficient or non-existent.

Traceability

Lack of coordination and deficient communication channels.

Lack of focus on documenting the implementation of ad hoc solutions.

Focus on service deployment, rather than on functional and security tests prior to implementation.

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

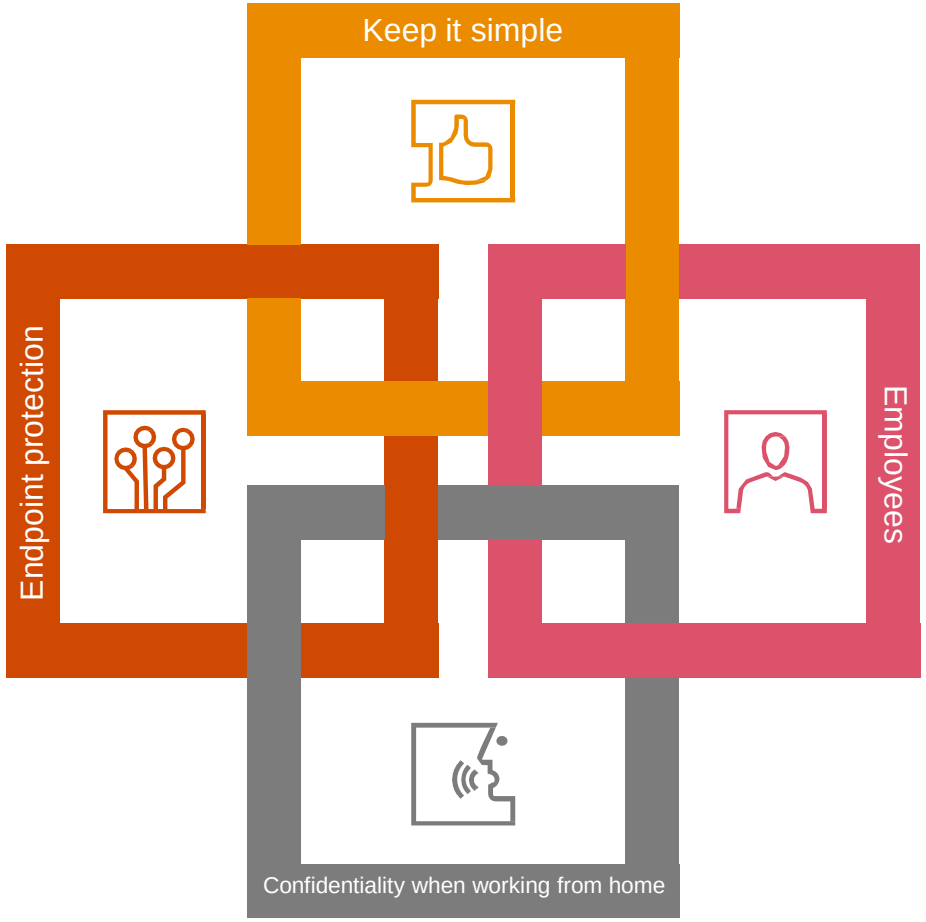
Company data may be visible to third parties looking at the physical device if the room layout or access protection is insufficient.

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.

2

Guidance

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 solutions

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.

Collaboration – 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.

Collaboration – 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.

Connectivity – 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.

Endpoints – 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

AWM Industry Leader
Oliver Weber
oliver.weber@pwc.com
+352 49 48 48 3175

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

AWM Risk Leader
Benjamin Gauthier
b.gauthier@pwc.com
+352 49 48 48 4137

AWM Tax Leader
Sidonie Braud
sidonie.braud@pwc.com
+352 49 48 45 469

AWM 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

AWM Assurance Leader
Michael Delano
michael.delano@pwc.com
+352 49 48 48 2109

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

Explanatory Notes

Asset & Wealth Management
May 2020

pwc

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: Portfolio, Operations & Data, Regulation Risk & Compliance as well as Investor Impact. Although regulatory and risk 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.
- Your normal PwC contacts are ready to assist you and involve our specialists to support your needs.

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.