

# ASIA PACIFIC REGULATORY WATCH

## **2020 Updates on Data Privacy**

*Data Protection regulatory updates  
for Singapore & Hong Kong*

## **BCBS Revision to the PSMOR**

*Principles for the Sound  
Management of Operational Risk*

## **Central Security Depository Regime reminder**

*Re-defining the rules for securities  
settlement*

## **RegTech Corner**

*Regulatory Lineage  
Focus on Solidatus solution*

# Foreword

It is our great pleasure to present the latest publication of Aurexia's Asia Pacific Regulatory Watch newsletter.

In this edition, our regulatory watch will be focused on hot topics that we consider as key to monitor in the unprecedented context: Data Management, Risk Oversight and Reporting Regulatory Compliance.

More than ever cyber attacks have substantially increased during the COVID-19 crisis and have urged regulators to reinforce their guidelines. PDPA and PDPO requirements have evolved to enable financial institutions to leverage on data opportunities while developing strong data protection framework. At the same time, the pandemic has also exacerbated operational risks, and triggered banks business continuity plans (BCP). This has highlighted the importance of operational resilience to ensure the safeguard of the financial system.

Furthermore, reporting requirements continue to present itself as a huge challenge for financial institutions. Securities Services are specifically impacted by CSDR (Central Security Depository Regime) regulation, for which the next milestone is targeted on the 22<sup>nd</sup> of November 2020.

If you have any comments, suggestions, or would like further details on any of the features included in this month's edition, please do not hesitate to contact us.



**Dominique HERROU**  
CEO – Senior Partner



**Sithi SIRIMANOTHAM**  
Partner APAC

# Contents



**2020 Updates on Data Privacy** 04  
Data Protection regulatory updates for Singapore & Hong Kong



**BCBS Revision to the PSMOR** 08  
Principles for the Sound Management of Operational Risk



**Central Security Depository Regime reminder** 12  
Re-defining the rules for securities settlement



**REGTECH CORNER**

**Solidatus** 16  
End-to end proof of data lineage to satisfy growing number of regulations

# Data Protection regulatory updates in Singapore



## Moving towards less restrictions on personal data usage but with heavier financial penalties for data breach

Eight years after the Personal Data Protection Act (PDPA) was first introduced in Singapore, the Parliament recently passed on 2<sup>nd</sup> November 2020, key amendments to the regulation.

As defined back in 2012, the PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data, where personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organization has or is likely to have access. PDPA recognizes both the rights of individuals to protect their

personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes.

As data is strongly becoming a key valuable asset in the digital economy, therefore PDPA amendments seek to keep Singapore’s data protection regulation aligned with evolving technology developments (such as Artificial Intelligence) and global regulatory trends (like GDPR). The PDPA regulatory changes will empower innovation, enhance products and foster Singapore’s attractiveness as a digital hub in APAC.

### PDPA key updates acted



**Data Breach Notification now mandatory**

Organizations are now required to inform both the Personal Data Protection Commission (PDPC) and affected individuals of data breaches that result in or are likely to result in significant harm.



**Heavier Financial Penalties**

Organizations that face data breaches will be exposed to fines up to 10% of annual turnover in Singapore (if organization's annual turnover in Singapore exceeds SG\$10 million), or SG\$1 million, whichever is higher. Financial penalties previously were capped at SG\$1 million.



**Expanded Consent Framework**

Deemed consent and exceptions to consent requirement: companies will be allowed to use, collect, and disclose personal data for "legitimate purposes" (business improvement, or a wider scope of R&D), without having to obtain consent from people. Existing consent exceptions were defined for investigations and emergencies purposes, they will now also be used to prevent fraud, enhance products and services, or conduct market research to target customer expectations.



**New right to Data Portability**

People will have higher autonomy over their personal data, enabling them to switch easily to new service providers. It will also foster development of new services and innovation as organizations will have more access to data. At the request of people, organizations must transmit an individual’s personal data that an organization has under its control, to another organization in a common machine-readable format.

## Heavier fines for data breaches, and more support for legitimate uses of data

Last year, the Personal Data Protection Commission (PDPC) investigated 185 cases involving data breaches and issued 58 decisions. It ordered 39 organizations to pay SG\$1.7 million in penalties, including the highest fines of SG\$750,000 and SG\$250,000, which were meted out to Integrated Health Information Systems and Singapore Health Services, respectively. Financial sector also accounts for part of these fines. For instance, Insurance company AIA was fined SG\$10,000 by the PDPC for mistakenly sending 245 letters meant for various customers to just two people which contained full names and policy numbers of intended recipients, as well as premium amounts and due dates.

More recently in August 2020, the Central Depository was fined SG\$32,000 after it mailed dividend cheques to outdated addresses, putting more than 200 account holders at risk of having their personal data disclosed.

The increased penalties that can be imposed by the PDPC of Singapore will likely bring compliance with

organizations. This is compounded with the mandatory data breach regime, which will require organizations to ensure they have the policies, procedures and processes in place to handle data breach incidents to meet the new requirements.

Given the current environment where there has been an increase in cyberattacks during the COVID-19 pandemic and the push by many organizations to digitize and engage in remote working, organizations should consider carefully the new regime and ensure they are well prepared should a cyberattack take place.

## Companies based in Singapore should now get ready to:

- Review existing data protection policies and procedures to ensure compliance with the upcoming changes to the PDPA
- Ensure that relevant agreements with external vendors or data third parties contain necessary undertakings and indemnities to protect the company's interests in case of a data breach
- Implement the necessary procedures and technical arrangements that will be needed to comply with the new data portability obligation



# Data Protection regulatory updates in Hong Kong



## Relying on GDPR proven best practices to reinforce PDPO framework locally

On 20<sup>th</sup> of January 2020, the Constitutional and Mainland Affairs Bureau (CMAB), and the Privacy Commissioner for Personal Data (PCPD), published the PDPO Review Paper to propose updates on Hong Kong's Personal Data Privacy Ordinance (PDPO) to the Legislative Council Panel on Constitutional Affairs.

The PDPO was passed in 1995 and is one of Asia's longest standing comprehensive data protection laws. It provides guidance to how data users should collect, handle and use personal data (information which relates to a living individual and can be used to identify that individual), and other provisions imposing further compliance requirements. The PDPO underwent major amendments in 2012 (resulting in the strengthening of restrictions on the use of personal data for direct marketing purposes) but remained unchanged since then.

The proposed Privacy Reforms represent a major

enhancement of personal data protection in Hong Kong, including strengthening of enforcement powers of the Privacy Commissioner.

Given handling and use of data is a critical aspect of all businesses, understanding and planning for the proposed reforms will be important for all businesses that operate in Hong Kong or collect personal data from Hong Kong.

Apart from data breaches, doxxing (find or publish personal data about an individual on the internet without permission) is another reason for the reform. Since 2019, the unauthorized public disclosure of people's personal data online has become increasingly common. From June last year, the PCPD has received or uncovered over 4,700 doxxing-related complaints.

Therefore a comprehensive reform and modernization of the legislation has become particularly important.



PDPO key updates under discussion



**Data Breach Notification now mandatory**

To setup a mandatory data breach notification mechanism. Currently no statutory requirement under the PDPO to notify the PCPD of a data breach (notifications are made on a voluntary basis under the existing regime).



**Heavier Sanctioning Powers**

To impose administrative fines (likewise GDPR) to be linked with the annual turnover of the data users and to raise the current criminal fine levels for the penalty for contravening an enforcement notice (currently HK \$50,000). As of today, the PDPO is empowered to issue enforcement orders, but not administrative fines for PDPO breach. A data user that contravenes the PDPO but complies with an enforcement order will not face an administrative fine.



**Expanded definition of Personal Data**

To expand the definition of "personal data" – from personal data relating to an "identified person" to personal data relating to an "identifiable person" - to increase scope of information subject to the PDPO.



**New data Retention Policy**

To make it mandatory for organizations to implement a clear data retention policy specifying the retention periods for different categories of personal data collected, as well as how the retention period is calculated. The PDPO currently only includes a general requirement that a data user take all practicable steps to ensure that personal data is not kept longer than necessary.



**New regulation of Data Processors**

To impose direct legal obligations on processors and sub-contractors to ensure a fair sharing of responsibilities between data users and processors and to ensure that processors and sub-contractors are accountable for failing to protect personal data. Currently the PDPO only directly regulates the processing of personal data by data users (commonly referred to as data controllers in jurisdictions such as the EU and Singapore).



**New regulation of doxxing activities**

To curb doxxing (deliberate and malicious posting of personal data of individuals online) by introducing specific powers for the PCPD to request removal of such content from online platforms, and to undertake criminal investigation and prosecution of such matters.

The PCPD has received and identified over 4,700 instances doxxing. 1,400 of these instances have been referred to the police for further investigation.

The proposed PDPO amendments aim to strengthen Hong Kong’s data privacy regulation and align it more closely with international data protection standards.

While these amendments are welcomed by the public, they will surely increase compliance costs for the private sector. Corporates and financial institutions should be prepared to introduce

appropriate measures to their systems and review their contracts with their data processors.

Though there is currently still no indicative timeline as to when any formal amendments may take place, companies should continue to monitor and update their privacy statements in line with international standards.

# Genesis of BCBS principles for the sound management of operational risk

## A revision to enhance operational risk management framework

**In 2003,** The Basel Committee on Banking Supervision introduced its Principles for the Sound Management of Operational Risk, and revised them in 2011 to incorporate the lessons learned from the financial crisis. In 2014, the Committee conducted a review of the implementation of the Principles. The purpose of this review was to assess the extent to which banks had well implemented the Principles, to

detect significant gaps in the implementation and to identify emerging operational risk management challenges not currently addressed by the Principles.

This review identified that some of the principles had not been adequately implemented within financial institutions, and that further guidance would be necessary to facilitate their implementation in the following areas:

### 2014 Outcomes



#### Risk Identification & Assessment

Risk identification and assessment tools guidances needed for: RCSA, key risk indicators, external loss data, business process mapping and the monitoring of action plans generated



#### Senior Management Oversight

Advice for board of directors and senior management to take the lead in establishing a corporate culture guided by strong risk management



#### Change Management

Change management programmes and processes guidances necessary to ensure their comprehensive, accurate and effective monitoring



#### Risk Appetite and Tolerance

Guidances for the appropriate definition and review of risk appetite and tolerance, that articulates the nature, types and level of operational risk the bank is willing to assume



#### Three Lines of Defence Implementation

Support needed to ensure the accurate implementation of the 3 lines of defence, especially by refining the assignment of roles and responsibilities



#### Risk Disclosures

Formal disclosure policy implementation support to determine what operational risk disclosures the bank will make and what are the internal controls necessary

**2020 Consultation** The committee recently also recognised that PSMOR principles did not sufficiently capture certain important sources of operational risk, such as those arising from information and communication technology. It is in this context that a proposed revision of PSMOR principles has been submitted for consultation in August 2020. The updated principles consequently cover Governance, Risk management environment, Information and communication technology, Business Continuity planning and the role of disclosure. It is highlighted that these elements should not be viewed in isolation. They should be integrated components of the operational risk management framework (ORMF) of the bank.



# 2020 key changes of BCBS principles for the sound management of operational risk

## Consultation of key changes based on 4 main areas

### Inclusion of ICT Risk in the principle 10:

The Committee introduces a dedicated principle for Information and Communication Technology risk. This principle highlights the necessity for banks to implement a robust ICT governance, consistent with operational risk appetite and tolerance. ICT risk should consequently be subject to appropriate risk identification, protection, detection, response and recovery programmes.

### Resilience removed from Business Continuity:

Recognising the increased risk for significant disruptions to bank operations from pandemics, natural disasters, cyber security incidents or technology failures, the Committee has developed specific principles for operational resilience.

### Other additional guidances have been provided on the following areas:



**Governance:** clarification provided on the responsibilities within the 3 lines of defence



**Risks:** importance of strong risk management approach and culture across all top risk categories highlighted



**Controls:** there is much more detail on internal controls best practices in several principles



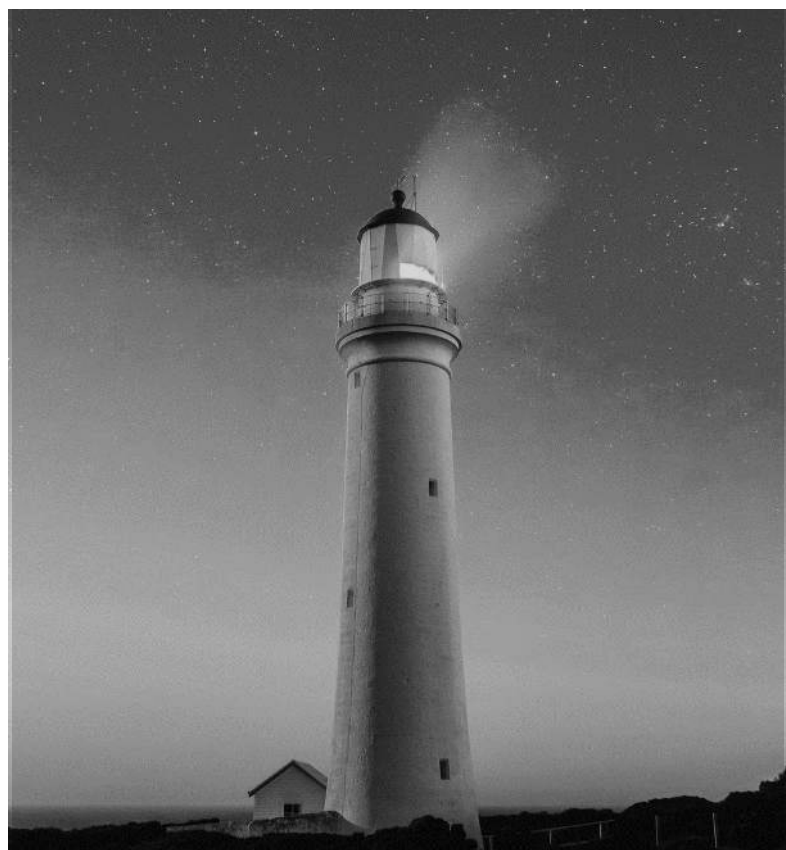
**Forward looking approach:** operational risk management should be forward-looking and change management should include risk assessment

### Risk Appetite Statements further guidances:

Principle 4 provides deeper details on Risk Appetite Statements, which should involve a large range of stakeholders, be clear, simple, easy to communicate and forward looking by aligning short - and long-term strategy.

### New requirement for banks to disclose exposure:

Principle 12 introduces that *“A Bank’s public disclosure should allow stakeholders to assess its approach to operational risk management and its operational risk exposure”*. This means that banks might ensure that disclosure, which has significantly increased these past years, does not impact the risk exposure.



# BCBS spin off on the principles for the sound management of operational risk

## Reasons for Operational Resilience specific principles

COVID-19 outbreak highlighted the importance for financial institutions to have a strong operational risk management framework. The Committee believes that *“further work is necessary to strengthen bank’s ability to face operational risk incidents, such as pandemics, cyber incidents, technology failures or natural disasters”* and consequently introduced principles for Operational Resilience to provide additional safeguard to the financial system.

Until this year, the most predominant operational risks that banks faced resulted from vulnerabilities related to the rapid adoption of and increased dependency on technology infrastructure for the provision of financial services and intermediation. The COVID-19 situation have increased economic and business uncertainty. Disruptions have affected information systems, personnel, facilities and relationships with third-party service providers and customers. In addition, cyber threats (ransomware attacks, phishing, etc) have taken more importance, and the probability of

operational risk incidents due to people, processes and systems has been exacerbated by the work from home requirement.

The Committee has defined the operational resilience as the ability of a bank to deliver critical operations through disruption. Operational resilience is made possible through key activities such as risk identification and assessment, risk mitigation by the implementation of a robust control environment, and by the monitoring work performed to minimize operational disruptions occurrence and impacts.

To be highlighted that the Committee recognises that *“many banks have well established risk management processes that are appropriate for their individual risk profile, operational structure, corporate governance and culture, and conform to the specific risk management requirements of their jurisdictions”*.

Principles for operational resilience are organized into seven identified categories aimed to provide best practices for financial institutions.

# BCBS spin off on the principles for the sound management of operational risk

## 7 new principles for Operational Resilience to be highlighted

Operational resilience principles are organized across seven categories: governance, operational risk management, business continuity planning and testing, mapping of interconnections and interdependencies of critical operations, third-party dependency management, incident management and resilient information and communication technology (including cybersecurity).



# Central Security Depository Regime reminder

## Re-defining the rules for securities settlement in Europe

The CSDR (Central Securities Depositories Regulation) implementation since 2014 has led to massive changes for all market players, from CSD participants (CCPs and Settlement agents) to all actors of the buy and sell-sides. This regulation aims at harmonising settlement standards and promote competition and improve settlement efficiency. Today, with the approaching implementation – Q1 2022 – of the settlement discipline regime (SDR), a component of CSDR focusing on the improvement of settlement efficiency, Aurexia has decided to issue its latest insights on SDR and its implications across financial services.

### Reminder on what is CSDR

The CSDR (Central Securities Depositories Regulation) is a European regulation No 909/20142 that redefine the rules for securities settlement in Europe. It aims to improve post-trade harmonization, safety, and efficiency, and enhance the legal and operational conditions for cross-border settlements by increasing efficiency. In other terms, the regulation’s goal is to provide shorter settlement periods and mandatory penalties for failed trades so that it could raise settlement rates from about 97.5% to more than 99% in Europe.

The regulation applies to European Central Securities Depositories (CSDs), their participants, and to securities settlement systems in the European Union (EU). Thus, the CSDR has a global applicability for financial institutions making settlements through a European Union exchange. The extra-territoriality impacts for APAC actors of the regulation highlighted in the next sections

### Main provisions of CSDR



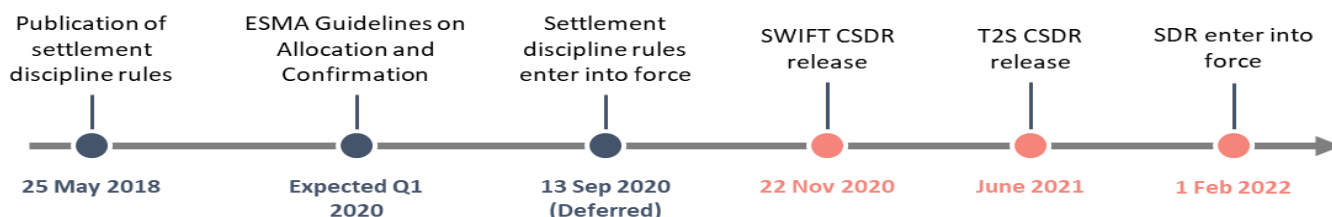
- 01. Creating a regulatory and prudential regime for central securities depositories
- 02. Increasing the robustness and resilience of securities settlement arrangements
- 03. Creating a single market for central securities depositories services

# Central Security Depository Regime timeline

## Multiple releases leading up to SDR entry into force by 2022

### Breakdown of the overall timeline

The regulation was published in the Official Journal in August 2014 and is gradually entering into force. The go live date has recently been deferred to February 2022 with the expected entry into force of settlement discipline rules (SDR).

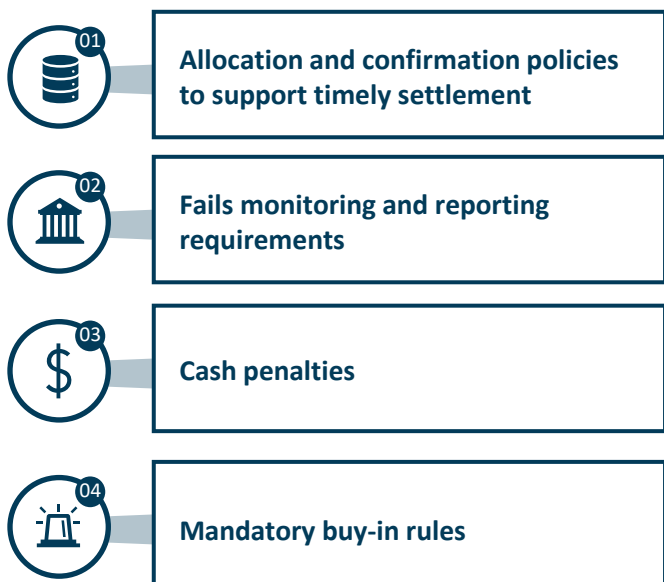


### SDR, the main component of CSDR entering into force early 2022

Its objective is to harmonize aspects of the settlement cycle and introduces new rules for cash penalties and buy-ins. It is designed to make settlements more efficient and will include cash penalties for trade fails.

In Asia, SDR primarily affects non-EU/EEA-domiciled trading entities such as asset owners, asset managers, broker-dealers, private banks, and wealth managers. As long as they or their clients trade European securities, the settlement discipline rules will apply to all transactions intended for settlement on a European CSD. This covers transferable securities, money-market instruments and UCITS; exemptions include shorter-dated securities financing transactions.

### Market participants and intermediaries will have to adapt at 4 different levels:



For instance, CSDs will be tasked with monitoring and reporting settlement efficiency rates and facilitating matching and related processes to support trouble-free settlement.

This means that CSDs will have to pass failed trade penalty charges on to their participants, i.e. the custodians or the broker-dealers. At the same time, mandatory buy-ins mean that companies are now legally obligated to buy-in a failing party should a transaction fail over a specific period.

# Central Security Depository Regime scenarii

## Examples of SDR scenarii impacting market participants

### Brief glimpse of the new reality

Under SDR, market participants deemed responsible by a CSD for a settlement-failure face cash penalty, calculated daily by the CSD. If not resolved within a specified time frame per instrument, a mandatory buy-in will come into effect. This will create further costs for the failing trading member, including appointment of a buy-in agent, and potentially higher market prices, to replace the original transaction. Additionally, high failure rates may cause longer-term reputational damage, harming relationships with counterparties.

#### The case of confirmation / allocation



The delay for settlement being fixed at T+2 signifies a need to ensure that all mandatory settlement information has been exchanged between the market participants at the earliest stage. Investment firms will require from their clients to provide them in the written allocation and confirmation all information needed to facilitate the settlement (e.g. the identification of the accounts to be used). Also, this information must be provided to the investment firms on T (trade day) or under certain condition before T+1 noon, to avoid any delay in the settlement process.

#### The case of penalties



A matched settlement instruction not fully settled on time will be penalized irrespective of the root cause of the non-settlement (lack of cash, lack of security, instruction matched after ISD, instruction put on hold, etc.). The penalty will be paid by the failing participant to the CSD and will be applied for each day the instruction fails to settle.

#### The case of buy-ins



When the financial instrument has not been delivered within a set period after the ISD, SDR imposes a mandatory buy-in process to close outstanding settlements. If the settlement fails, this process mandates the buyer to source the securities elsewhere, cancel the original instruction(s) and settle with the new counterparty. The difference (if any) arising from the net costs of the original transaction and the buy-in transaction, will be passed onto the original failing party. However, the buyer (purchasing counterparties) cannot rely on the CSD or Stock Exchange infrastructure to handle the buy-in process for them. They will have to execute buy-ins by appointing an execution of buy-in agent. In case the buy-in agent fails to provide the securities, a cash compensation procedure may be used.

# Central Security Depository Regime challenges

## Challenges to face following the entry of SDR

Addressing new changes – From exposure assessment to operational readiness



### Exposure assessment

In the coming months, it is important that firms to SDR and prepare for its implementation. For many, the first 2 priorities will be on estimating their risk by:

- 1) Finding out the level of exposure to EU markets in terms of concentration of assets in the region
- 2) Assessing the level of fails and tackling underlying causes




### Operational readiness

At the same time, market participants need to reassess their operational/technical readiness regarding their settlement efficiency by:

- 1) Engaging with clients and counterparties on process changes to accommodate penalties and buy-ins
- 2) Establishing dispute resolution procedures

Stakeholders likely to make changes in one or more of the following processing areas:

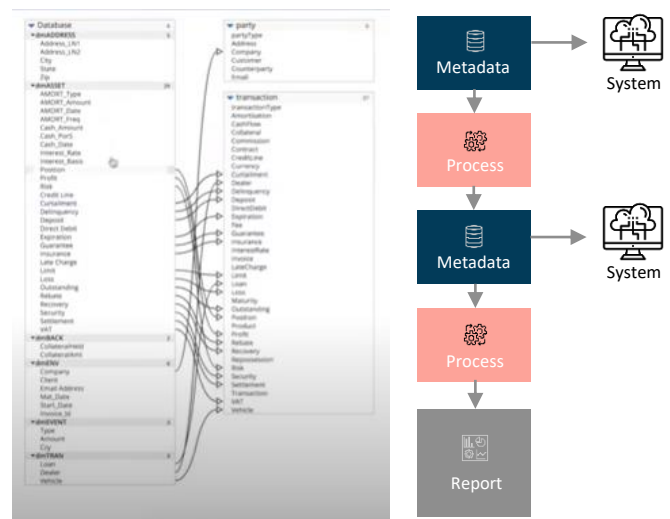
Stakeholders	Examples of processing areas impacted (Non-exhaustive)
 <p>Asset owners, managers, broker-dealers, other intermediaries, and custodians</p>	<p>All firms buying and selling EU securities must have clear supervision over their entire securities processing transaction chain from pre-trade to execution to post-trade processes, including settlement and payment.</p>
	<p>Existing post-trade processes will have to be reviewed to assess fails ratios and identify the causes of trade fails. Firms may look to redirect their transaction flows toward counterparties and service providers with most stable settlement operations.</p>
	<p>Some clients of securities buyers in Asia may become beneficiaries of failed trade penalties. Thus, they must review their processes to validate fails-related communications, and challenge penalties (if any) by providing the documented evidence.</p>
	<p>If a receiving party needs to find a buy-in agent to source the replacement securities before passing the cost to the failing party, it will have to face potential short supply of existing agents due to multiple regulatory requirements</p>
	<p>Invoicing processes may have to be reassessed at the level of payments related to settlement discipline costs. Industry working groups are exploring potential repapering needs.</p>



**END TO END PROOF OF DATA LINEAGE TO SATISFY GROWING NUMBER OF REGULATIONS**

Since 2008, the world has seen a marked unshift in regulation across many sectors. This has put, in turn, a great deal of stress on the financial services industry, with a lot of money and intellectual capital being spent to ensure regulatory compliance. The challenge now is to return to the new norm of being able to satisfy the regulators and also allow financial services to react to quick changes.

Solidatus is a key part of the solution, knitting and consolidating the data economy to collaborate, take care of critical data elements and to free up time. Solidatus focuses primarily on the increasingly regular and critical theme of data lineage. Only after an organisation understands its data, and its data provenance, can it begin to consolidate and harmonize. Solidatus allows organisations to provide detailed and complex data lineage in a visual form that provides a richness and depth of detail that other reporting methods cannot.



Data Lineage Process

**SIMPLE TO USE**



The intuitive and simple web interface is easy to use and requires little training.

**EASY ACCESS**



Solidatus is a browser-based application and it can be up and running in the cloud in minutes.

**IDENTIFY MISSING DATA**



Immediately start modelling and easily identify where additional discovery is required.

**ACCELERATED DISCOVERY**



Accelerate discovery by sharing parts of the models to identified system experts to fill in the detail.

Solidatus is used to:

- **REGULATE:** Be proactive rather than reactive towards regulatory requirements including BCBS239, CCAR, DFS504 and GDPR.
- **TRANSFORM:** Understand the organisation’s data flow in order to plan change, analyse its impact and future-proof the data ecosystem.
- **GOVERN:** Coordinate, control and plan change throughout an enterprise regardless of the type of system, the data in use, where it is or who owns it.
- **OPTIMIZE:** Reduce redundancy and misuse of data by ensuring that all data is catalogued and owned, with the correct lineage to easily spot anomalies;





**Dominique HERROU**

*CEO – Senior Partner*

[dominique.herrou@aurexia.com](mailto:dominique.herrou@aurexia.com)

+65 8313 6610

**Sithi SIRIMANOTHAM**

*Partner APAC*

[sithi.sirimanotham@aurexia.com](mailto:sithi.sirimanotham@aurexia.com)

+65 8876 0186

## Bringing value, Together

© 2020 Aurexia Pte Ltd. Material in this publication may not be copied, reproduced or republished in any way except for your own personal, non-commercial use. Prior written consent of Aurexia Pte Ltd must be obtained if you intend to reuse. The contents of this publication represent the views of Aurexia and should not be taken as advice or the provision of professional services in any way.

Aurexia Pte Ltd is a Private Limited company registered in Singapore. Aurexia Pte Ltd is part of the global Aurexia group, which also has offices in France, Luxembourg, London and Hong Kong.

# Aurexia



Bringing value, together