Agenda
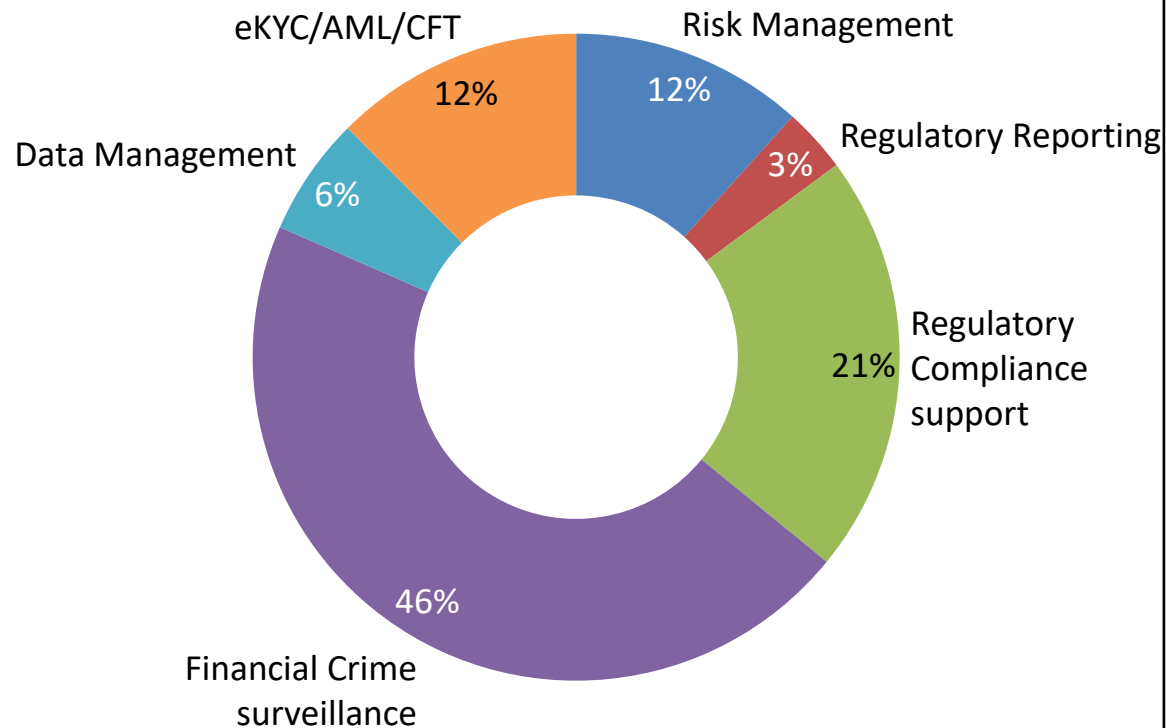
Regtech & Suptech Trends

Regtech Case Studies & Survey Findings

Suptech Case Studies & Survey Findings

Recommendations

Regtech & Suptech technologies are playing a big role in enabling financial service providers to comply and regulators to manage risk

Key Regtech & Suptech segments in 2019

- eKYC/AML/CFT 12%
- Risk Management 12%
- Regulatory Reporting 3%
- Regulatory Compliance support 21%
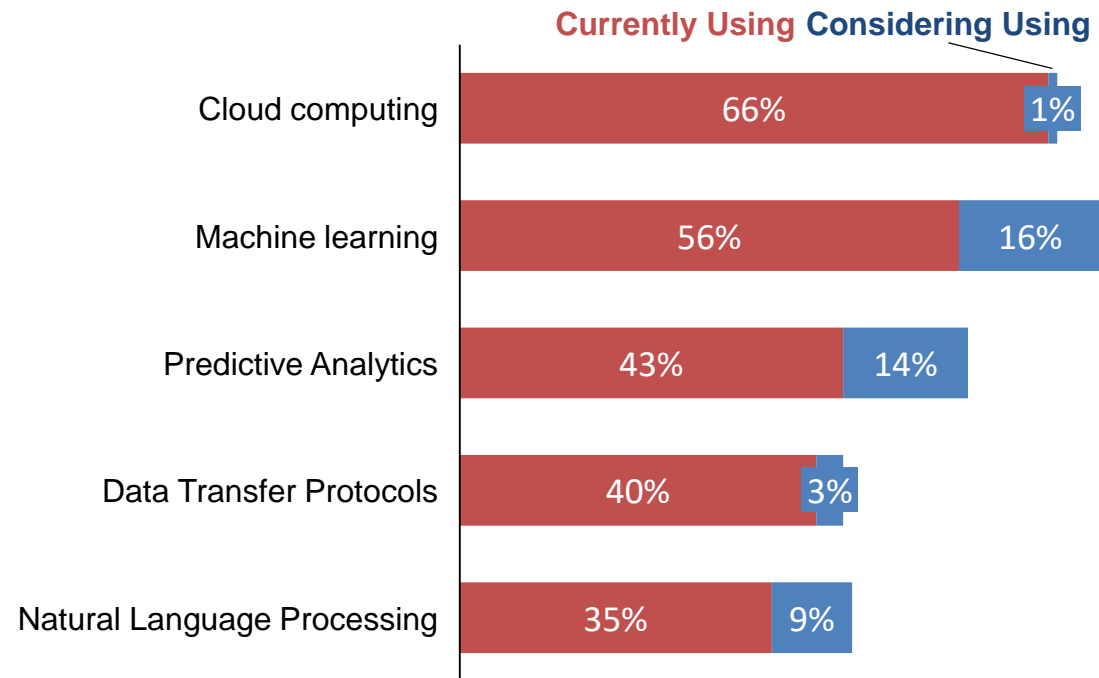- Financial Crime surveillance 46%
- Data Management 6%

Top Regtech & Suptech use-cases in 2019

- **Cryptocurrency regulation** is one of the key areas Regtech is expected to impact. Regtech enables analysis of digital crypto transactions, identification of suspicious activity, and sophisticated anti-money laundering monitoring.

- **AI for fraud detection** is another area where Regtech has grown rapidly owing to vast amounts of data becoming digitized and computing power being stronger than ever. As a result Regtech players are increasingly deploying AI technology solutions that are able to detect fraud at scale through detecting patterns in structured and unstructured datasets with a higher level of accuracy.

- **Identity verification** is another fast growing area owing to Know Your Customer (KYC) laws requiring banks to verify identities, assess customer risk factors. Regtech enables automated processes to analyze high-risk individuals or entities and verify identities through comprehensive databases, ensuring higher accuracy and consistent recommendations.

SOURCE: Deloitte Consulting 2019 Regtech Report

There are various technologies enabling Regtech & Suptech

Top 5 Technologies Employed in Regtech & Suptech offerings

Currently Using **Considering Using**

Technology	Currently Using	Considering Using
Cloud computing	66%	1%
Machine learning	56%	16%
Predictive Analytics	43%	14%
Data Transfer Protocols	40%	3%
Natural Language Processing	35%	9%

SOURCE: Cambridge Centre for Alternative Finance Report 2019

- About two thirds (66%) of the sector delivers its offerings through the **cloud**, with 56% of vendors employing **machine learning** and 43% using **predictive data analytics** to describe patterns or predict behaviours.

- Over a third(35%) use **natural language processing** (NLP) to parse regulatory content.

- In proportion, the use of **machine learning** and **data analytics** is set to grow further and could be used by nearly three quarters of vendors if current predictions are correct.

- Looking forward, however, it is voice recognition, **Distributed Ledger** Technology (DLT) and **Geographic Information System** (GIS) mapping that are likely to make the biggest gains from current levels.

Globally, several Jurisdictions have already introduced successful Regtech initiatives to drive better risk management and regulatory compliance

Financial Conduct Authority (FCA)	Hong Kong Monetary Authority (HKMA)	Australian Security and Investment Commission (ASIC)	Financial Service Regulatory Authority (FSRA)	Superitendencia Finaciera de Columbia (SFC)

- In UK, the FCA implemented a **TechSprint event and a proof of concept on turning regulations into machine-readable format** was demonstrated.

- In Hong Kong, the HKMA announced a several **initiatives aimed at supporting banks' day-to-day risk management or regulatory compliance processes** as way to scale development and adoption of Regtech

- In Australia, ASIC received federal government funding to develop programs that **position Australia as a world leader in developing and adopting Regtech solutions that support risk management and compliance** problems relating to financial services.

- UAE government launched an **initiative led by the FSRA to develop a blockchain-based, electronic Know Your Customer (KYC)** solution.

- SFC launched **"Proyecto Regtech" programme to promote the local development of Regtech** in collaboration with third parties.

Globally, several jurisdictions are deploying Suptech solutions to enhance their supervision efforts

Monetary Authority Singapore (MAS)	Financial Conduct Authority (FCA) and Bank of England	Australian Security and Investment Commission (ASIC)	National Bank of Rwanda (NBR)

- Singapore is one of the market leaders in Suptech having launched a **data analytics system** to search through the 3,000 monthly Suspicious Transaction Reports (STR) on money laundering and terrorist financing risks that financial institutions file with MAS

- FCA and Bank of England are also one of the global leaders in begun exploring the potential for **machine readable and executable regulations** (MRERs), including through a TechSprint event hosted in November 2017.

- Australia actively rolling out Suptech initiatives to enable supervision of capital markets using public/private partnerships.
  - Example is the **Market Analysis and Intelligence (MAI) system** used for market surveillance of the Australian capital markets

- Rwanda has also began rolling our suptech initiatives with their flagship **automated data pull project** to enable supervisors to access raw data from supervised FSPs' systems and then process the data into reports using its own software.

Agenda

Regtech & Suptech Trends

Regtech Case Studies & Survey Findings

Suptech Case Studies & Survey Findings

Recommendations

Four main areas of Regtech use-case development

	1 Regulatory compliance	**2** Risk Management	**3** Financial Crime	**4** Identity Management
Description	Compliance reporting entails Regtechs tools with offerings that helps financial institutions in gathering **regulatory intelligence**, **mapping policies**, **compliance governance** and **automated data sharing** with regulatory authorities.	Regtech tools with offerings that help FSPs detect **market risks**, monitor **employee conduct** for suspicious behavior and protect data from numerous **cyber risks**.	Regtech tools with offerings that help FSPs monitor financial transactions in real-time to detect **fraud**, **market abuse**, **money-laundering** or **terrorist financing activities.**	Regtech tools with offerings that help FSPs with **Know Your Customer (KYC) procedures**, **anti-money laundering sanctions and anti-fraud screening.**
Activities	• Compliance and governance • Regulatory reporting • Regulatory intelligence	• Market risk • Conduct risk • Cyber risk	• Financial Fraud • Money Laundering and Terrorism financing • Market abuse	• KYC for identity verification • KYC for onboarding • KYC for AML checks
Examples	Enterprise-wide solutions for identifying and keeping track of changes in regulatory requirements, at local or global levels, and solutions for automated real-time monitoring of compliance levels and compliance risk.	Tools to improve the risk management process at financial institutions, by bringing efficiencies to the generation of risk data, risk data aggregation, internal risk reporting, automatically identifying and monitoring risks etc..	Solutions that offer real-time transaction monitoring and auditing, such as by using DLT, end-to-end integrity validation, anti-fraud and market abuse identification systems, back-office automation and risk alerts.	Digitalization of client or partner onboarding processes, digitization and sharing of customer/partner information, gathering and analyzing customer and transaction data, and identifying suspicious transactions and customer/partner profiles.

WaymarkTech

Regtech is being deployed to carry out compliance management leveraging on AI and other technologies

Waymark helps tier 1 and 2 UK based global banks to maintain awareness and understanding of ALL regulations

Overview

- Waymark Tech is a London based Reg-Tech and Sup-Tech firm offering Regtech solutions.
- The firm develop and provide software services using advance AI and NLP for tier 1 & 2 United Kingdom based global banks and investment firms and advisory firms with clients facing complex regulatory demands, as well as public sector organisations involved in defining and monitoring regulations.

How it works

- Waymark's Scanning capability utilises AI technology to continually monitor and analyse regulatory changes, alerting firms to new regulations, or changes to regulations, and making recommendations to ensure compliance.
- The Regulatory Intelligence platform brings a variety of complementary information together and analyses it, using a mixture of algorithmic techniques, with the human in the loop.
- Waymark also utilises Amazon Web Services (AWS) cloud architecture to establish collection, processing, search and review of regulatory data source(s).
- Waymark deploys unique NLP and machine learning technology to tag the content.

Key Outcomes

- The tool reduce the time and money Compliance teams spend on regulatory monitoring.

- The in-built Tracking capability can monitor, flag and remind individual colleagues to review an alert, capture their actions, monitor progress.

- Waymark can link to the client's existing change management platform via API for complete integration of services.

Regtech is also being deployed to carry out KYC procedures

IDmission helps financial institutions around the world conduct onboarding of clients

Overview

- IDmission enables fully compliant digital onboarding solutions that use AI to detect fraud risks and eliminate them.
- It offer technologies for digital account opening, digital Identity validation and digital account access.
- IDmission has created a software development kit (SDK), named eVolv, which financial institutions can directly integrate with their mobile applications.
- The kit is being used by institutions such as Western Union, KZB Bank, Afore Azteca the pension fund and many more financial institutions around the world to carry out their clients onboarding activities.

How it works

- Once implemented, the tool enables the organisation to captures data such as ID Documents, biometrics, video recording, video conferencing, GPS location and more, to ensure KYC processes are complete.
- By assessing all of these data types, the company can meet KYC requirements for any jurisdiction around the world.
- It is also able to support any ID document through face, fingerprint, iris and voice biometrics.
- It also guarantees the liveness of individuals and stops biometric deduplication by matching all new customers with the existing database.

Key Outcomes

- Fully compliant digital onboarding solutions that use AI to detect fraud risks and eliminate them.

- Smooth customer acquisition and account opening resulting in the improvements in customer convenience.

- Reduction in risks including fraud, money laundering and associated identity risks.

- Opening an opportunity for millions of people to enter the financial sector.

DATAVISOR

Regtech tools are also being used in financial crime surveillance

DataVisor AI fraud prevention platform

Overview

- DataVisor is an AI fraud prevention platform that detects AML behavior including mule accounts, layering, and structuring that are typically used to avoid detection by traditional fraud and money laundering solutions.
- It can identify fraudulent accounts even when a fake install is camouflaged with real looking user activity.
- Its human understandable rules enable businesses to reduce their manual review time and be meet compliance requirements.
- The rules are created on a daily basis and are constantly monitored and updated or deprecated. The engine is back testing enabled.

How it works

- DataVisor intelligent fraud prevention platform uses unsupervised machine learning
- It helps FIs handle application and transaction fraud, promotion abuse, money laundering, fake accounts, account takeovers and credit scams
- Its full stack risk platform predicts emerging attacks by identifying bad actor accounts while they are in incubation stage and provides end to end protection against attacks by modern cybercriminals

Key Outcomes

- Keep companies and their customers safe from fraud and abuse.
- The integration of rules engine and machine learning technologies allows users to address fraud with comprehensive tools while removing the complexity of fraud management.
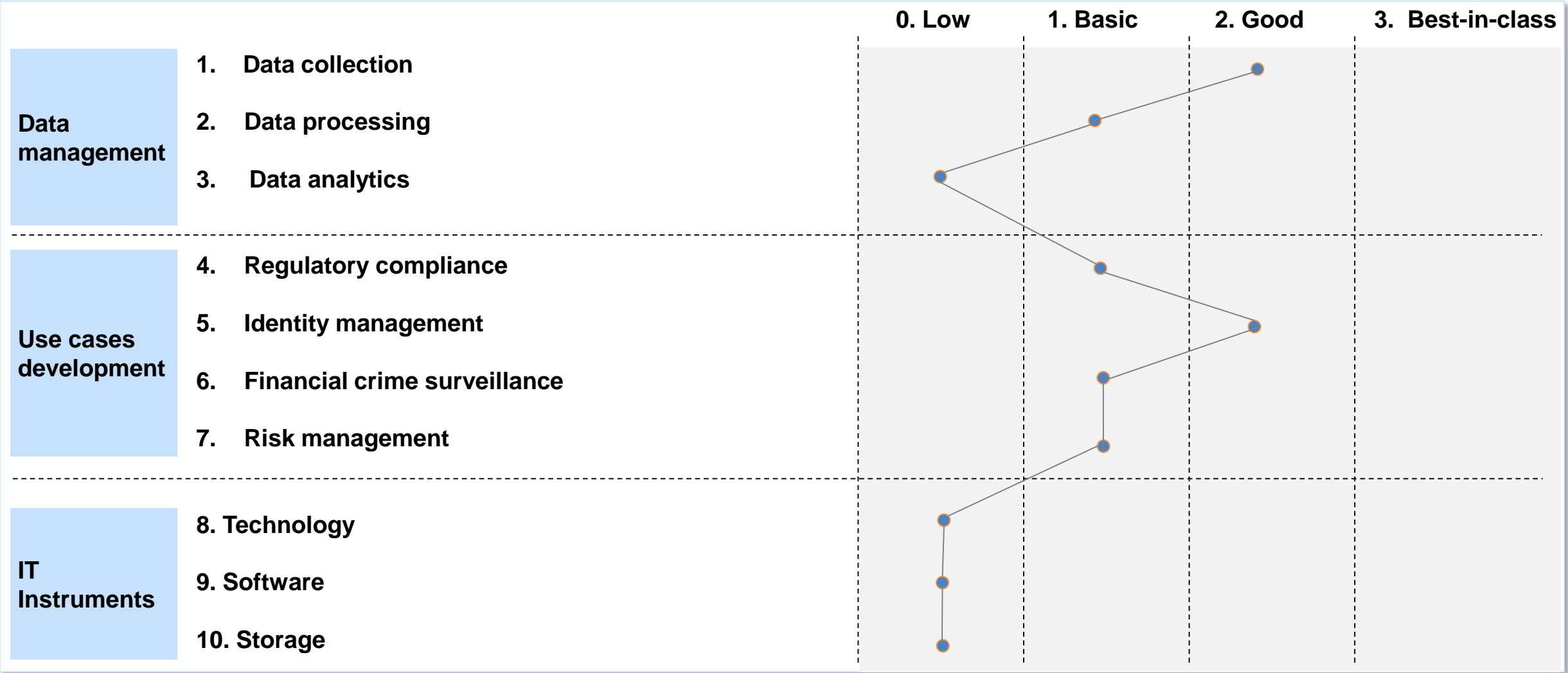
Highlights and Challenges from SA industry survey

Highlights

- **Enhanced efficiency, capacity, and speed** of compliance

- By **making compliance less complex and capacity-demanding, Regtech solutions could free up capital** for more productive uses.

- **Reduction in cost of hiring** expensive compliance talent pool by outsourcing key functions.

- **End-to-end data management** with a granular view of insights.

- **Lower cost of some technology solutions**, e.g. the benefit of cheaper cloud-based services.

Challenges

- FSPs are finding it **difficult to find people with relevant technology skillsets and deep domain-specific knowledge**

- FSPs tend to **focus on revenue generating viewing compliance as a cost function**, thus relegating it to a lower priority level.

- **Solutions offered by Regtech providers are often difficult to scale** across various departments of an FSP.

- **Fears around sustainability and financial stability of Regtech startups** and ability to offer long-term service

- Regtech implementation **requires costly and often untested technologies** such as AI/ML, RPA

- While promising, **uncertainties still remain around Regtech's credibility and impact.**

Agenda

Regtech & Suptech Trends

Regtech Case Studies & Survey Findings

Suptech Case Studies & Survey Findings

Regtech Case Studies & Survey Findings

Two main types of Suptech use case development

	Investigative Suptech	Preventative Suptech
Description	▪ Investigative Suptech entails detection of regulatory non-compliance after its manifestation. This regulatory breach is within a spectrum that can range from mild flaws to severe.	▪ Preventative Suptech on the other hand, implies allowing the supervisor to act in advance of a breach of regulation by any of the supervised entities, thereby monitoring the risk factors that could trigger a breach.
Activities	▪ Misconduct analysis ▪ Data Management ▪ Reporting	▪ Risk monitoring ▪ Financial Crime Surveillance ▪ Identity Management
Technologies	▪ **Machine learning (ML):** ML assist with data quality, validation and analytics. ▪ **Cloud computing:** allows for greater and more flexible storage of data. ▪ **Data lakes:** Provides scalable storage solution for diverse structured, semistructured, and unstructured data**.** ▪ **Natural language Processing (NLP):** NLP and ML analyse suspicious transactions and money laundering networks.	▪ **Neural networks:** Neural networks can be used to detect liquidity risks. ▪ **AI/ML**: AI/ML techniques can be used in the identification of macro-financial risk and to accurately process, verify, and authenticate identities at scale. ▪ **NLP:**NLP is being used to measure market sentiment. ▪ **Heat maps**: heat maps are also being used to highlight potential financial stability issues**.**

Suptech is also being used to conduct financial crime surveillance

Mexico AML data storage and analytics tools

Overview

- The Comisión Nacional Bancaria y de Valores (CNBV), Mexico's national banking and securities commission, is charged with supervising its financial system.
- CNBV has reengineered its data infrastructure to strengthen its AML supervisory capacity and to accommodate a growing Fintech sector.
- The core of the new data infrastructure developed in collaboration with R2A and Gestell, is a central access controlled data storage platform that can house transactional data submitted by supervised entities via **APIs.**

How it works

- Once securely stored, the platform renders the data in risk dashboards, alerts, and statistical reports using **Machine Learning models**, **advanced data** analytics, and **cutting-edge visualization tools** (e.g., algorithms and notifications).
- It identifies outliers (suspicious transactions, clients, or reports, including risk factors that are not visible to the human eye) and informs and targets on-site visits.
- Previously, the CNBV lacked an efficient means to extract insights from existing data since supervisors often had to upload appropriate data from compact discs and paper files, and analyze them in **Excel spreadsheets**.

Key Outcomes

- The system reduce **compliance costs.**
- Enable CNBV to improve **AML-related data validation** and **augment analytical capabilities using ML**.
- Increase the **volume**, **granularity**, and **frequency** – and improve the quality – of **AML related data**.
- The new solution allows the CNBV to reduce **inefficiencies** and **generate deeper intelligence**, **making AML supervision more risk-based**.
- Enable CNBV to retrieve and mine historical records.

Suptech initiatives are being used to conduct risk monitoring

Risk monitoring Suptech tools across various jurisdictions

Overview

- **De Nederlandsche Bank (DNB**) uses Suptech applications in identifying signals of emerging risks in the financial system using massive amounts of data from FMIs, such as payment systems.
- **The United States Security and Exchange Commission** use of Natural Language Processing (NLP) to measure market sentiment to assess the tonality of registrant filings. Together with topic modelling, the tonality signals are converted into risk measures using ML algorithms.
- **The Federal Reserve**, the **European Central Bank** and the **Bank of England,** for example, use "**heat maps"** to highlight potential financial stability issues.

How it works

- The researchers at the **DNB** convert the massive amount of transactions processed into risk indicators by applying traditional **econometric methods** to their data, developing algorithms to pick up relevant transaction types, developing indicators based on globally defined principles for financial market infrastructures and machine learning.
- The **Bank of England** derive heat maps from automated analyses of daily and other data (such as stress tests) being produced by supervised entities.

Key Outcomes

- The system reduce **compliance costs**.
- Improved **off-site risk monitoring** that allows for better and earlier detection of potential risks.
- More **efficient information flows** between providers and supervisors, between consumers and supervisors, and across supervisors
- Integration of **structured and unstructured data**, thus making analyses richer.
- Enhanced supervisory capability by making possible the humanly impossible
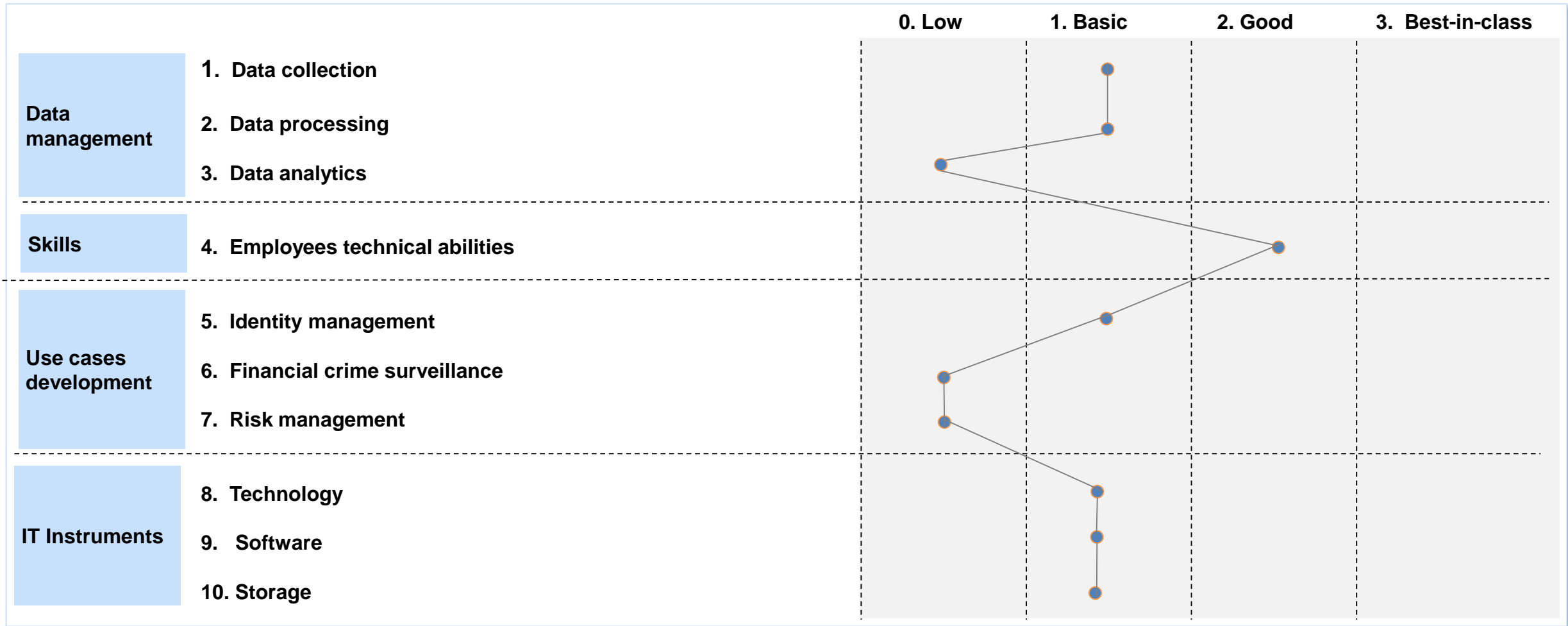
Summary of Highlights and Challenges from SA regulators

Highlights

- Suptech applications **enhance effectiveness** by improving on traditional or manual processes, thereby allowing for faster supervisory action.

- Suptech applications **reduce costs** by automating processes that typically used to involve several people.

- Suptech applications **enhance supervisory capability** by making possible the humanly impossible. Securities markets supervisors, for example, receive thousands of regulatory filings from supervised entities. It is impossible for supervisors to review each one closely.

- Suptech leads to **Improved consumer outcomes** (better protection, increased confidence in market).

- Suptech tools **brings in larger share** of financial sector under supervision.

- Suptech **enables** and **enhances** risk-based supervision (better identification and measurement of risk.

Challenges

- Supervisory agencies working with Suptech encountered **data quality issues**. Data quality and completeness can be an issue for non-traditional sources of information (e.g. social media).

- Finding the **right talent** is a key challenge and key person risk is high when it comes to Suptech.

- Lack of **funding or budgetary constraints** to be able to deliver the Suptech tools.

- Technical issues relate to **computational capacity** constraints **and lack of transparency on how some technologies work**.

- There is a heightened operational **risks that comes with Suptech tools adoption, e.g. cyber-risk**, which highlight the need for improved risk management in supervisory agencies when using Suptech applications.

- Supervisory agencies need to adhere to the standard rules and policies applicable in their jurisdictions when undertaking Suptech projects.

Agenda

Regtech & Suptech Trends

Regtech Case Studies & Survey Findings

Suptech Case Studies & Survey Findings

Recommendations

Based on global best practice, it is proposed that the IFWG launch a Hackccelarator focused on Regtech, Suptech, and Digital Capabilities

Key Objective

Leverage our proximity and access to emerging Financial technology (Fintech) firms through the 'Innovation hub' to collaborate with disruptive technology players to accelerate Regulators' digital transformation efforts

Use-Case Focus Areas

Regtech	Suptech	Digital Tools & Capabilities
▪ Regulatory Reporting	▪ Real time monitoring	▪ AI/Machine learning/ NLP
▪ Risk Management	▪ Market surveillance	▪ Block chain/ DLT
▪ Identity Management & Control	▪ Misconduct analysis (AML/CFT, Fraud)	▪ Robotic process automation (RPA)/ Intelligent automation (IA)
▪ Compliance	▪ Forecasting & predictive analytics	▪ Collaboration technologies
▪ Transaction Monitoring	▪ Risk signaling (credit, liquidity)	
	▪ Virtual assistance	

A staged process will be implemented to foster Regtech, Suptech, & Digital innovation across IFWG Regulators

	1	**2**	**3**	**4**	**5**
Stage	REGULATOR AND INDUSTRY USE-CASE SURVEY	HACKATHON LONGLIST	HACKTHON SHORTLIST (DEMO-DAY)	PROTOTYPING	LAUNCH & SCALE SOLUTION
Detail	• Conduct Survey/Interviews with regulators and industry players to gauge need, maturity, and prioritization of Regtech, Suptech, & digital use-cases • Publish synthesized list of priority use-cases identified by regulators	• Invite Innovators to apply for Hackathon • Leverage SMEs to Review and shortlist most promising solutions for DEMO DAY	• Identified **Fintech/ Digital firms to Showcase & Demo their technologies** to relevant IFWG business units (IT, Supervision etc) • **IFWG Business units to select most promisng innovations that they'd like to further test for implementation**	• **Fintech to perform a limited non-binding pilot test with an interested regulators** to test effectiveness and benefits of the technology	• If tests and pilot is successful **commercial agreement** is negotiated and entered into with technology firm • **Technology solutions embedded and scaled** across IFWG regulators
Timing	Annually	Bi-Annually	Bi-Annually	As-Needed	As-Needed

Successful execution of Regtech, Suptech, and Digital Hackccelerator depends on four key enablers

Resources
- Market intelligence on emerging Fintech & Digital
- Innovation facilitation, Event Management, Digital transformation & commercialization skills
- Budget

Digital ambition
- Support and willingness to innovate/trial/test/experiment from Regulatory Leaders
- Alignment across IFWG members on key digital, regtech & suptech priorities/agenda and timing

Partnerships & Ecosystems
- Build and maintain relationships with cutting-edge technology firms and ecosystem
- Innovation-friendly procurement approach
- Seamless onboarding/integration of partners

Operating model
- Agile way-of work
- Rapid development and go-to-market

Regtech & Suptech Hackccelerator

Activity	2020						2021											
	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Communication: ▲ IFWG Present (Sep), ▲ Video Series (Oct), ▲ Video Series (Nov), ▲ Video Series (Dec)

Search: Survey, Shortlist (Jan–Feb), Shortlist (Jul 2021)

Demo: Startup Demo Prep (Mar–Apr), ▲ Demo Day 1 (May), Startup Demo Prep (Aug–Sep), ▲ Demo Day 2 (Oct)

Prototype: Prototying (Jun–Jul), Prototying (Oct–Dec)

Launch: Deployment & Scaling (Aug–Dec)

Appendix:
Additional Slides

Survey Findings Details: Regtech

Data collection `Good`

- The survey results indicates that majority of FSPs have **automated** their data collection process, followed by those using combination of **manual** and **automation process.**

Regulatory compliance `Basic`

- Regulators are leveraging **inhouse build solutions** and technologies tools such as, **Sentine**l, **Law explores**, **SAS enterprise case management, Lexus Nexus** and **etc.**

Technology `low`

- Survey results revealed that very few , FSPs has **big data architecture** with **AI** enabled solutions to support compliance.

Data processing `Basic`

- Majority of the FSPs are using the combination of **manual** and **build-in data validation** rules into the systems to process the data.

Identity management `Good`

- For KYC purposes, most FSPs are making use of **inhouse built solutions**, some prominent technology tools such as, **Finger biometrics**, **World check**, **Lexus nexus**, **facial recognition** and others.

Storage device `low`

- Majority of FSPs interviewed are still storing their information **inhouse**.
- Very few are making use of **cloud** service and those who are using it, is in combination inhouse storage device.

Data Analytics `Low`

- Most FSPs interviewed indicated that they are able to conduct **descriptive** and **diagnostics analytics**, while a small number of them are able to conduct **descriptive, dignostics, prescriptive and predictive analytics.**

Risk Management and financial surveillance `Basic`

- To conduct financial crime surveillance most FSPs are using **inhouse built software tools** and **external vendors solutions**, while for risk management **SAS** and other **advanced statistical tools** are being mostly used.

Software `low`

- Results also indicates that large number of FSPs are not using prominent technology tools such as SQL data mining, Python script, AI tools, advance statistics tools such as SAS, R,MATLAB to support compliance.

Survey Findings Details: Suptech

Data collection `Basic`

- Majority of regulators are using combination of manual, bulk (web) uploads and automated reporting to feed data into their systems.
- Almost all regulators are having plans/ strategies in place to enhance their data management processes.

Identity Management `Basic`

- Regarding identity management, majority of the regulators are using the combination of inhouse technological tools and prominent technological tools such as GoAML, SAS to conduct KYC procedures, AML, as well as sanctioning and fraud screening.

Technology `Basic`

- Most regulators are in the transition from digitilisation and automation of certain manual processes to data stack architecture supporting Big data technology and AI.

Skills `Good`

- Majority of regulators are having small teams of data scientists and there are moves/plans by almost all the regulators interviewed to move towards expanding the teams and build more data science skills sets .

Data processing `Basic`

- Most regulators have built-in data validations rules in their systems to process and validate the data.

Risk monitoring `Low`

- Regulators are using simple descriptive statistics techniques to monitor risk with.
- The use of AI and its subsets e.g. ML to conduct risk monitoring, is at a very low level.

Storage devices `Basic`

- Almost all the regulators are storing their data inhouse and on alternative physical sites. There is a desire to move to cloud storage services but they sounding caution pointing at issues of sovereignty of the state.

Data Analytics `Low`

- Regarding analytics capabilities, the majority of regulators are currently only able to conduct descriptive analytics.

Financial Crime Surveillance `Low`

- Processes to conduct financial crime surveillance most organisations have inhouse built software tools that assist them to investigate AML/CFT, fraud and other financial crimes.

Software `Basic`

- Majority of regulators are using software tools e.g. (SAS), Oracle, Power BI, Magic, Python scripts etc., for data manipulation and there are plans to adopt AI tools in future. However, the use of these tools to support supervision in very minimal.

Suptech tools are being deployed to carry out regulatory reporting and compliance

Central Bank of Philippines (BSP) application programming interface and prudential reporting and visualisation application

Overview

- BSP in collaboration with the Regtech for Regulator Accelerator(R2A) has developed **Compliant Risk Technology (CRT)** an **Application Programming Interface(API)** and back office **reporting** and **visualisation** application to allow financial institutions to submit high-quality, granular data digitally and automatically to BSP with higher frequency.

How it works

- The system enable BSP staff to make **data validation** and **analysis** by generating customized reports for supervisory and policy development purposes in different formats and near-real time.
- Previously the BSP's Supervisory Data Center (SDC) team received incomplete, late, and or inconsistent reports.
- Data cleaning and validation consumed significant resources and e-mailing compliance reports was inherently insecure.
- The quantity of available data that was actually analysed was limited as the collection, validation, and mining process was primarily manual and resource intensive.

Key Outcomes

- The model ensures more **consistent** and **higher-quality data**.
- Automation allowed for **consistent and timely submission**, which dramatically reduces penalties for late or erroneous submissions.
- Automation also **improved the data validation process** by detecting duplicate submissions.
- The project **reduces compliance costs** significantly and assists BSP in generating timely, crisper insights on the Philippine financial sector
- **Data security has dramatically improved** since automated communications are secured with industry-standard encryption

OeNB
OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

In regulatory reporting we are witnessing a shift to automated reporting, data quality management and dynamic compliance by FSPs

Automated data collection in Austria

Overview

- The Austrian central bank (OeNB), in collaboration with Austrian banks, has developed an innovative **data-input regulatory reporting platform** that provides a direct interface between the IT systems of the central bank and banks.
- The platform allows banks to upload data in a standardized format, according to Austrian central bank requirements and specifications.
- The central bank can then transform the data into **smart cubes**, or data sets, containing specific data and information relevant for different departments within the Austrian central bank.

How it works

- Banks feed data into basic datacube at Austrian Reporting Service (AuRep).
- This represents a single, complete description of the reporting data that is redundancy-free and contains harmonised definitions.
- Consecutively, a set of standardised transformation rules convert the data in the basic datacube in such a way that it can be pushed to the OeNB.

Key Outcomes

- The model ensures more consistent and higher-quality data.

- It relieves banks from having to prepare different reports for different supervisory departments.

- Allows cost sharing of compliance between the supervisor and industry.

- Reduces data management and monitoring requirements and time in implementation of regulatory requirements.