DIGITAL
TRANSFORMATION
SOLUTIONS

SUPTECH TAXONOMY

5 September 2025

WWW.DTSOLUTIONS.IO

THE SUPTECH TAXONOMY

The SupTech Taxonomy is a comprehensive classification system that organises supervisory use cases (the "sup" in suptech) and the technologies and data science tools used to support them (the "tech").

It draws a clear distinction between *supervisory functions* and *technological enablers* to methodically identify the needs of financial authorities, organise the digital tools that address those needs, and establish a structured framework for aligning supervisory challenges with fit-for-purpose solutions.

The taxonomy comprises **16 supervisory domains**, subdivided into **163 distinct use cases**, structured hierarchically around the core activities and processes carried out by supervisory authorities. Each use case represents a practical application of supervision, mapped to relevant risks, mandates, and institutional objectives.

On the technology side, the taxonomy classifies tools and capabilities based on their functional application across the five layers of the **supervisory DataStack**—a conceptual architecture used to describe how data is ingested, managed, analysed, acted upon, and safeguarded in the supervisory context.

By decoupling supervision from technology and then linking them through structured mappings, the SupTech Taxonomy offers a practical, modular, and forward-looking framework for suptech development, assessment, and strategic planning.

FINANCIAL SUPERVISION

- Anti money laundering, counter financing of terrorism and proliferation financing (AML/CFT/CPF) supervision
- Artificial Intelligence (AI) use by regulated firms - supervisory oversight
- Capital market, securities and investment instruments supervision
- Competition monitoring
- Compliance assistance
- Climate/ESG risks supervision
- Consumer protection and market conduct supervision
- Cyber risk supervision
- Digital assets/cryptocurrencies oversight
- Financial inclusion and equity monitoring
- Insurance supervision
- Licensing and authorisations
- Open banking and open finance supervision
- Operational risks supervision
- Payments oversight
- Prudential supervision of banks and non-bank deposit taking institutions

TECHNOLOGY - DATASTACK

- Data Collection
- Data Processing + Validation
- Data Storage
- Data Analytics
- Data Products

DIGITAL TRANSFORMATION SOLUTIONS

1 FINANCIAL SUPERVISION

DIGITAL TRANSFORMATION SOLUTIONS

1 FINANCIAL SUPERVISION

Anti money laundering, counter financing of terrorism and proliferation financing (AML/CFT/CPF) supervision

USE CASE	DEFINITION
Offsite supervision support (automated)	Use of data analytics and automation to support AML/CFT/CPF-focused supervisory examinations and investigations.
Risk-based CDD/KYC assessment	Evaluate institutions' customer due diligence and KYC processes using entity matching, risk scoring, and address verification, in line with a risk-based approach.
Suspicious activity detection	Detect, classify, and monitor suspicious transactions or patterns using rule-based or machine learning techniques.
Misconduct pattern detection	Analyse data on misconduct related to AML, fraud, market abuse, or mis-selling to identify supervisory concerns and emerging risks.
Metadata intelligence	Analyse metadata associated with reports submitted to the Financial Intelligence Unit (FIU), including submission patterns, completeness, and frequency, to identify anomalies or gaps.
Policy and training document review	Analyse supervised institutions' internal policies (e.g. CDD, beneficial ownership) and training materials to assess adequacy and alignment with regulatory expectations.
Derisking analysis	Assess the drivers and impacts of derisking by financial institutions, including the criteria used and the consequences for access to financial services (e.g. geo-tagged account closures, sector drop-offs).
Onsite AML/CFT examination	Conduct in-person inspections of institutions to assess AML/CFT/CPF compliance, governance, and risk controls.
Supervision of designated non-financial business or professional (DNFP)	Oversee AML/CFT/CPF compliance of DNFBPs such as real estate agents, casinos, lawyers, and accountants, including reporting obligations and risk controls.
Risk scoring of institutions	Assign risk scores to institutions based on behaviour, reporting, exposure types – supports prioritisation of supervisory attention.
PEP/sanctions screening validation	Review institutions' name-screening systems (e.g. false positives, list usage, screening gaps).
STR/CTR quality review	Assess the quality, consistency, and proportionality of STR/CTR submissions across institutions. Identify under-reporting, over-reporting, duplication, or incomplete filings to prioritise supervisory follow-up and improve AML/CFT reporting standards.

DIGITAL TRANSFORMATION SOLUTIONS

1 FINANCIAL SUPERVISION

Intelligence (AI) use by regulated firms - supervisory oversight

USE CASE	DEFINITION
Model validation and explainability	Assess the transparency, fairness, and explainability of AI/ML models used in credit scoring, fraud detection, trading, etc.
Bias and discrimination detection	Evaluate models for potential unfair treatment or disparate impact across population segments (e.g. gender, race, geography, income) using disaggregated data and fairness metrics.
Consumer outcome monitoring for AI-powered services	Track consumer-facing outcomes (e.g. loan rejection rates, pricing anomalies, dispute resolution patterns) associated with AI-powered processes, to detect harmful or unintended effects.
Governance and accountability of AI systems	Assess the existence and effectiveness of internal AI governance frameworks within regulated entities—including model documentation, review committees, model risk rating, change logs, and override protocols.
Audit trail and traceability validation	Verify whether institutions maintain auditable records of AI model decisions, training data, and tuning processes—especially in high-impact use cases (e.g. surveillance, underwriting).
Monitoring AI use in high-risk or opaque areas	Identify and supervise the use of black-box or untested AI systems in high-risk functions (e.g. algorithmic trading, automated insurance claims, robo-advice), where decision opacity or speed may outpace governance.
Third-party AI model and data provider oversight	Supervise the outsourcing of AI solutions, especially where institutions use external models or datasets from unregulated vendors.
Robustness and adversarial risk assessment	Evaluate AI systems for robustness under stress, including resilience to adversarial manipulation (e.g. synthetic identity fraud, manipulated inputs).
Regulatory reporting and model inventory requirements	Require financial institutions to maintain AI model registries and submit periodic reporting on model use, updates, performance, and risk level.

1 FINANCIAL SUPERVISION

Capital market, securities and investment instruments supervision

USE CASE	DEFINITION
Market manipulation detection	Detect unusual trading patterns that may indicate manipulation, including spoofing, layering, or wash trades.
Insider trading detection	Identify transactions that may have exploited material non-public information, using trade timing, access logs, and event correlation.
Poor disclosure detection	Identify delayed, incomplete, or misleading disclosures from listed companies, including financial statements, material announcements, and risk reports.
Onsite inspection	Conduct onsite inspections of securities firms, broker-dealers, and other capital market participants to assess compliance and risk controls.
Derivatives contract analysis	Analyse reported derivatives contracts to assess exposure to market risk and compliance with regulatory thresholds or margining rules.
Risk-based prioritisation	Use entity, product, or behaviour risk metrics to prioritise supervisory reviews and interventions.
Data handling	Manage secure ingestion, integration, and remote access to capital market data, including cloud-based systems and multi-source data harmonisation.
Suitability and mis-selling detection	Analyse sales practices and customer profiles to flag unsuitable product distribution or excessive churn.
High-frequency trading (HFT) pattern analysis	Detect latency arbitrage, quote stuffing, or other HFT-related risks.
Bond issuance and rating surveillance	Monitor public and private bond issuance, default trends, and rating transitions.
Cross-market and cross-border surveillance	Detect arbitrage or manipulation strategies that span jurisdictions or asset classes.

1 FINANCIAL SUPERVISION

Competition monitoring

USE CASE	DEFINITION
Market concentration and competition analytics	Monitor overall market structure and competition dynamics using metrics such as market share, concentration indices (e.g. Herfindahl-Hirschman), and firm performance—informing supervisory analysis of pricing, market power, and barriers to entry.
Pricing and fees monitoring	Monitor product pricing and fees across institutions to detect outliers, abusive practices, or signs of reduced competition.
Price dispersion analysis	Detect pricing anomalies across institutions for similar products – flags possible collusion, lack of competition, or unfair pricing.
Market entry and exit trend analysis	Analyse firm entry and exit patterns to assess barriers to entry, innovation dynamics, and overall market attractiveness.
Merger and acquisition oversight	Assess proposed mergers and acquisitions for potential anti-competitive effects, including monopolisation, market foreclosure, and consumer harm.
Market power abuse detection	Identify anti-competitive behaviours such as predatory pricing, tying/bundling, or exclusionary practices.
Switching and portability friction analysis	Analyse consumer account switching patterns, porting requests, and associated costs/delays to identify lock-in or market stickiness.
Data-driven assessment of regulatory barriers	Use application/licensing data, sandbox performance, and firm exit surveys to quantify regulatory or operational barriers to entry.

1 FINANCIAL SUPERVISION

Compliance assistance

USE CASE	DEFINITION
Digital compliance guidance	Deliver rule-based or AI-assisted guidance to regulated entities to clarify compliance requirements in real time (e.g. via portals, chatbots, or embedded rule engines).
Automated compliance audits	Conduct automated checks of institutions' submissions, operations, or systems against regulatory requirements using predefined rules or workflows. May be embedded in a Regulatory Information System (RIS).
Standardised reporting automation	Generate automated, standardised reports from regulatory data to assist entities in meeting compliance reporting requirements.
Machine-readable regulations	Convert legal texts into structured, machine-readable formats (e.g. XML, JSON) to support digital compliance tools and automate regulatory change detection and impact assessment.
Regulatory obligations mapping	Help entities map specific obligations to their business lines, products, or internal controls—manually or via semantic tools.
Compliance self-assessment tools	Provide interactive checklists, dashboards, or AI-powered forms that enable institutions to assess and report on their own compliance status

1 FINANCIAL SUPERVISION

Climate/ESG risks supervision

USE CASE	DEFINITION
ESG exposure and risk identification	Collect and analyse ESG and sustainable finance data to classify exposures and assess climate and sustainability-related risks at firm or portfolio level.
Green financial market monitoring	Monitor developments in sustainable finance markets, including volumes, pricing, taxonomy-aligned products, and compliance with green labelling or verification standards.
Climate scenario analysis and stress testing	Apply climate-related scenarios (e.g. transition, physical risks) to assess the potential impact on institutions' portfolios and capital adequacy under various time horizons.
ESG portfolio alignment and risk analysis	Assess financial institutions' portfolios for alignment with ESG objectives (e.g. net zero), transition risks, and exposure to environmentally or socially harmful sectors.
ESG disclosure supervision	Collect and evaluate the quality, completeness, and reliability of ESG-related disclosures, including non-financial reporting on governance, environmental risks, and social metrics.
Greenwashing risk detection	Detect inconsistencies between ESG claims and underlying business models, investments, or activities—through text analysis, rating divergences, or data mismatch.
Climate-related risk transmission mapping	Map how climate and environmental risks may propagate through the financial system via correlated exposures, geographies, or sectors
ESG data gap and quality analysis	Assess coverage, granularity, and reliability of ESG data available to both supervisors and regulated entities. Helps design better reporting regimes and identify disclosure weaknesses.

1 FINANCIAL SUPERVISION

Consumer protection and market conduct supervision

USE CASE	DEFINITION
Complaints referral, tracking, and resolution	Facilitate consumer complaint submissions and manage resolution workflows, including escalation and feedback.
Real-time complaints monitoring	Use real-time dashboards and automated alerts to flag spikes or anomalies in complaint volumes or topics.
Complaints trend analysis	Analyse complaint data to identify systemic issues, emerging risks, or recurring service failures across the market.
Credit reporting complaint and rectification	Facilitate consumer complaints regarding credit reports and ensure correction of inaccurate records.
Alternative dispute resolution	Facilitate structured, non-judicial resolution of disputes between consumers and financial service providers.
Targeted misconduct detection	Detect misconduct in advertising, promotions, or sales practices, especially when targeting vulnerable groups.
Predatory pricing detection	Identify pricing strategies that exploit consumer vulnerability or intentionally undercut competitors to force market exit.
Consumer fraud detection	Detect and prevent fraud schemes targeting consumers, including identity theft, phishing, or deceptive products.
Misleading or poor disclosure detection	Identify and assess instances where pre-contractual or contractual information is incomplete, misleading, or unfair.
Terms and disclosure validation	Automatically review terms & conditions, privacy policies, and consent notices for clarity, fairness, and regulatory compliance.
Sales incentive scheme monitoring	Detect incentive structures within institutions that may promote misconduct, mis-selling, or unsuitable product distribution.
Dark pattern detection	Detect design patterns in apps or websites that nudge users toward decisions not in their best interest (e.g. hidden opt-outs, default traps).
Algorithmic auditing	Evaluate AI/ML systems used in customer-facing processes for bias, error, or unfair outcomes.
Web and social media sentiment analysis	Analyse consumer sentiment from digital channels (e.g. social media, forums) to detect dissatisfaction or emerging concerns.
Vulnerable consumer profiling	Identify patterns of disproportionate harm to specific groups (e.g. elderly, youth, women, rural populations) using complaints and usage data.
Risk-based peer group classification	Classify providers into risk categories based on consumer outcomes, conduct indicators, and systemic relevance.
Early warning systems	Use predictive models and multi-source data to detect consumer protection risks before harm materialises.
Comparative analysis of market entities	Compare behaviour and risks across different institutions or providers in a given sector.
Internal supervisory data integration	Analyse and integrate consumer protection data across departments (e.g. licensing, enforcement, compliance) to improve oversight.
Market conduct onsite examinations	Conduct field inspections of providers to assess compliance with consumer protection rules.

1 FINANCIAL SUPERVISION

Cyber risk supervision

USE CASE	DEFINITION
Cybersecurity risk assessment	Evaluate financial institutions' cyber risk exposure, control maturity, and vulnerability posture using internal reporting, supervisory questionnaires, or external testing results.
Audit trail verification and analysis	Review and validate digital audit trails to detect suspicious activity, support forensic investigations, and verify data integrity.
Cybersecurity compliance monitoring	Monitor adherence to cybersecurity regulatory requirements, including policies on governance, authentication, data protection, incident response, and business continuity.
Cybersecurity onsite inspection	Conduct on-location reviews to assess cyber risk controls, penetration test results, response capabilities, and compliance with supervisory expectations.
Threat intelligence integration	Leverage internal and external threat intelligence to identify emerging cyber risks across supervised institutions.
Third-party cyber risk supervision	Assess exposure to cyber risks arising from outsourcing, vendor platforms, or cloud service providers.
Incident reporting and follow-up	Track, analyse, and act upon cyber incident reports submitted by regulated entities.

1 FINANCIAL SUPERVISION

Digital assets/cryptocurrencies oversight

USE CASE	DEFINITION
Digital asset data ingestion and management	Ingest and manage structured and unstructured data related to virtual assets, wallet activity, and VASP operations from on-chain and off-chain sources.
Automated validation of crypto-related data	Automatically validate the structure, completeness, and plausibility of data submitted by VASPs, exchanges, and custodians.
Automated compliance checks for virtual asset providers	Perform automated audits of virtual asset service providers (VASPs) to assess adherence to licensing, AML/CFT, transaction monitoring, and reporting requirements.
On-chain network analysis	Conduct broad analysis of blockchain activity to identify systemic trends, illicit typologies, or anomalies across jurisdictions or asset types.
Transaction-level tracing and wallet forensics	Trace on-chain transactions and wallet linkages to detect illicit activity, fund flows, or ownership structures.
Cross-border coordination and intelligence exchange	Enable secure sharing of intelligence and supervisory data across jurisdictions for joint monitoring, investigations, and enforcement involving virtual asset actors.
Token issuance and whitepaper monitoring	Monitor token issuance platforms and review whitepapers for fraud risk, compliance gaps, and unsubstantiated claims.

1 FINANCIAL SUPERVISION

Financial inclusion and equity monitoring

USE CASE	DEFINITION
Monitoring financial inclusion outcomes across population segments	Track disaggregated financial access and usage indicators—by gender, geography, income, age, or firm size—to identify underserved groups and inform proportionate supervisory strategies. This includes monitoring account ownership, digital payment adoption, agent coverage, rejection rates, dormancy trends, and service quality.
Gender and equity impact analytics	Analyse inclusion and equality outcomes for priority segments (e.g. women, rural populations, youth, MSMEs) using data from regulated entities, surveys, and open sources to inform supervisory action or policy coordination.
Simplified CDD and tiered KYC supervision	Assess the implementation, effectiveness, and risk mitigation of simplified CDD and tiered KYC measures for promoting inclusion without compromising AML/CFT safeguards.
Geospatial analysis of financial access, usage, and risks	Use geospatial tools to analyse access gaps and infrastructure distribution, including distance to access points, regional service disparities, or agent activity.
Consumer education	Track and assess the reach and effectiveness of financial education and awareness campaigns, including communication clarity and audience engagement.
Consumer trust analysis	Analyse consumer trust, satisfaction, and perception of fairness using data from chatbots, complaints, surveys, and social media sentiment.
Disaggregated outcomes monitoring in supervision	Integrate sex-, age-, geography-, or income-disaggregated metrics into risk-based supervision models and peer classifications.
Over-indebtedness risk analysis	Detect patterns of excessive or harmful credit uptake in underserved groups, using complaints, bureau data, and loan performance.
Supervisory coordination with financial inclusion policy bodies	Use suptech tools to align supervisory insights with national inclusion strategies, financial service providers licensing reforms, or digital public infrastructure planning.

1 FINANCIAL SUPERVISION

Insurance supervision

USE CASE	DEFINITION
Insurance data ingestion and management	Manage structured and unstructured supervisory data related to insurers, intermediaries, and policies.
Automated insurance compliance checks	Automate audits of insurer filings and operations using workflow systems (e.g. RIS) to detect non-compliance.
ORSA supervision and analytics	Collect and analyse Own Risk and Solvency Assessments (ORSAs) submitted by insurers as part of enterprise risk review.
Automated validation of insurance data	Automatically check reported data for consistency, completeness, and compliance with validation rules.
Insurance sector stress testing	Conduct quantitative analysis of insurers' resilience under adverse scenarios, including macroeconomic and catastrophe risks.
Intermediary registration and licensing	Oversee the authorisation and registration of agents, brokers, and other insurance intermediaries.
Fit & proper assessment	Evaluate the integrity, competence, and qualifications of individuals in key positions (directors, shareholders, officers).
Insurance product filing and approval	Review and approve insurance products submitted for regulatory approval, including terms, pricing, and marketing.
Insurer risk profiling	Conduct risk-based assessments of licensed insurers, including solvency, governance, claims ratios, and exposure trends.
Insurance onsite inspection	Conduct field inspections of insurers and intermediaries to review compliance, controls, governance, and risk management.
Claims performance and conduct analytics	Analyse claims settlement practices to assess efficiency, fairness, consumer outcomes, and fraud detection.
Real-time digital supervision of insurers	Monitor insurers' public digital channels (web, social media, filings, news) to detect emerging risks and conduct violations.

1 FINANCIAL SUPERVISION

Insurance supervision

USE CASE	DEFINITION
Digital guidance for licensing and authorisation	Provide dynamic, automated guidance to applicants based on business model or product characteristics, including licensing routes, documentation, and regulatory expectations.
Automated pre-screening or eligibility self-check	Allow applicants to assess their eligibility before submission using decision trees or AI chatbots.
Automated processing and risk assessment of licence applications	Automatically process, score, and route licence applications using business model risk classification, data completeness checks, and workflow automation.
Risk-based post-licensing monitoring	Set up initial supervisory profiles and alert thresholds once a licence is granted—based on application data.
Digital licence registry and status tracking	Provide a digital registry with licence status, conditions, and supervisory history accessible to both regulators and the public.
Fit & proper assessment	Evaluate the integrity, competence, and qualifications of individuals in key positions (directors, shareholders, officers).

1 FINANCIAL SUPERVISION

Open banking & open finance supervision

USE CASE	DEFINITION
API availability and latency monitoring	Real-time monitoring of open banking APIs for uptime, speed, and errors to detect market conduct and resilience risks.
Consent management compliance	Supervisory analytics on user consent logs to detect non-compliance or data misuse by regulated or third-party entities.
TPP authorization and behavior monitoring	Detect unauthorised access, anomalous activity, or regulatory breaches by third-party providers.
Data-sharing quality and access fairness	Monitor whether data-sharing obligations are being fulfilled equitably across institutions and third-party participants.
Cross-sectoral supervision coordination	Enable inter-agency information sharing (e.g. financial, competition, data protection authorities) for ecosystem-wide risk detection.
API availability and latency monitoring	Real-time monitoring of open banking APIs for uptime, speed, and errors to detect market conduct and resilience risks.

1 FINANCIAL SUPERVISION

Operational risks supervision

USE CASE	DEFINITION
ICT/operational resilience assessment	Monitor compliance with ICT risk frameworks (e.g. DORA), including continuity planning, incident logs, and recovery timelines.
Third-party / outsourcing risk analytics	Analyse concentration and risk exposures to critical third-party providers (e.g., cloud, regtech vendors).
Incident reporting and impact analysis	Analyse supervisory incident reports (e.g. cyber events, outages, fraud events) for root cause, recurrence, and systemic impact.
Operational risk loss data monitoring	Ingest and benchmark reported losses related to fraud, IT failure, internal control breaches, etc.
Conduct culture and HR data analysis	Analyse staff churn, whistleblower activity, or misconduct patterns that signal deep-rooted operational weaknesses.

1 FINANCIAL SUPERVISION

Payments oversight

USE CASE	DEFINITION
Real-time payments volume and value monitoring	Monitor transaction volumes and values across payment systems to detect anomalies, bottlenecks, or operational risks in real time.
Cross-border payments monitoring	Track the performance, speed, cost, and reliability of cross-border payments in line with G20 targets.
Retail payment fraud surveillance	Analyse suspicious patterns in fast retail payments to detect fraud risks or system abuse.
Payment infrastructure performance analytics	Monitor uptime, latency, throughput, and failure rates of payment system components (e.g. RTGS, ACH, card networks).
RTGS stress simulation and risk modelling	Simulate shocks and stress scenarios on the RTGS system to assess liquidity risk, throughput disruption, and systemic spillovers.
Payment system resilience assessment	Monitor and assess the operational resilience of payment infrastructures, including BCP testing, interdependencies, and incident response readiness.
Interoperability assessment	Evaluate the interoperability of payment platforms (e.g. mobile wallets, QR-based systems, banks) to ensure open access and systemic efficiency.
Instant payment scheme oversight	Supervise the deployment, risks, and fairness of real-time retail payment platforms.

1 FINANCIAL SUPERVISION

Prudential supervision of banks and non-bank deposit taking institutions 1/2

USE CASE	DEFINITION
Cross-validation of regulatory submissions	Automated integrity checks across time periods, entity reports, and linked datasets to ensure data quality.
Automated prudential reporting	Generate reports on risk and compliance (e.g. CCP margins, exposures) using supervisory datasets and analytics workflows.
Interdepartmental analysis	Analysis of supervisory data across different departments within the authority to support integrated oversight and decision-making.
Cross-entity analysis	Cross-entity analytics (stacking multiple data sources), e.g. linking credit, liquidity, governance datasets across entities.
AI-assisted judgement review	Use of NLP or machine learning to assist in evaluating board meeting minutes, supervisory letters, or firm submissions.
Forecasting	Forecasting economic indicators (e.g., inflation, credit growth) and firm-level risks (e.g., default probability, provisioning needs) using predictive modelling and analytical tools
Peer-group/risk classification	Identification of peer groups and classification of institutions based on risk indicators, business models, or systemic relevance.
Threshold breach monitoring	Monitor for breaches in key prudential indicators (e.g., CAR, LCR, NPL ratio), triggering alerts or review.
Sectoral credit monitoring	Monitoring credit trends within economic sectors to identify emerging risks or credit concentration.
Borrower rating movement tracking	Tack changes in borrower ratings across institutions to detect deteriorating credit or regulatory arbitrage.
Investment patterns analysis	Detect trends and risk concentrations in the investment portfolios of supervised institutions.
Basel compliance analytics	Monitoring Basel III/IV requirements (capital, liquidity, leverage) across institutions.
Risk aggregation dashboarding	Real-time supervisory dashboards that integrate prudential, conduct, and systemic indicators across entities.
Offsite surveillance automation	Combine structured data (regulatory reports) and unstructured signals (media, social, filings) to support continuous risk surveillance.
Business model risk detection	Use structured and unstructured data (e.g., filings, digital footprints, product mix) to detect unsustainable or high-risk business models.

1 FINANCIAL SUPERVISION

Prudential supervision of banks and non-bank deposit taking institutions 2/2

USE CASE	DEFINITION
Risk-based prioritisation	Use of ratings, scoring models, and analytics to determine supervisory priorities based on institutional risk profiles.
Automated credit risk review	Analyse credit underwriting practices, risk grading, and provisioning adequacy using loan-level data and machine learning.
Liquidity risk supervision analytics	Analyse liquidity ratios (e.g., LCR, NSFR), funding concentration, and maturity mismatch to assess resilience.
Fit & proper assessment	Assessment of the fitness and propriety of directors, senior officers, and significant shareholders of supervised entities.
Supervisory planning analytics	Tools to prioritise supervisory activities, schedule inspections, and allocate resources based on evolving risk profiles.
Onsite examination	In-person inspections conducted at supervised institutions to assess compliance, governance, risk management, and controls.
Governance risk assessment	Automated analysis of board minutes, composition, tone, and behaviour to detect governance risks, conflicts of interest, and weak internal controls.
Supervisory policy impact analysis	Assess the outcomes of past supervisory interventions using outcome-based indicators and comparative analysis.
Scenario analysis	Evaluate the impact of hypothetical shocks or policy changes—such as climate risks, geopolitical instability, or cyber events—on institutions or markets. Typically narrative-driven and used to inform planning and policy responses.
Stress testing	Simulate institutional or system-wide resilience under extreme but plausible financial or economic shocks. Quantitative tool used to assess capital adequacy, liquidity, and solvency under adverse conditions.
Contagion and interconnectedness analysis	Identify how risks spread across institutions or markets through interlinkages such as interbank exposures, common asset holdings, or operational dependencies. Supports macroprudential oversight and early warning.
Systemic risk monitoring and macro-financial surveillance	Network analysis of cross-institutional exposures and identification of systemic vulnerabilities
Resolution planning	Evaluation of recovery plans, stress simulations, bail-in feasibility.
Early warning systems	Machine learning models to identify risk escalation patterns in past failures and flag emerging concerns.

2 TECHNOLOGIES

DATASTACK LAYER

DIGITAL TRANSFORMATION SOLUTIONS

2 TECHNOLOGIES | DATASTACK LAYER

Data collection

USE CASE	TECHNOLOGY	DEFINITION	GENERATION
File servers	Shared drives (e.g., SharePoint, Google Drive, Dropbox)	Cloud-based storage platforms that allow multiple users to store and share files.	1G
	Secure File Transfer Protocol (SFTP)	A secure network protocol for transferring files over a reliable data stream.	2G
Web portals or other document management	Web portal	A website interface that provides ability to manually upload documents and other regulatory reporting.	
Application programming interfaces (APIs)	Push API	Sends data to the receiving system automatically when an event occurs.	3G
	Pull API	Allows the receiving system to request or "pull" data at regular intervals.	
Advanced collection (e.g., scraping, streaming, or AI-based)	Chatbots	AI-based systems that simulate conversation to collect or provide information.	4G
	Web scraping (e.g., Scrapy, BeautifulSoup)	Automated methods to extract data from websites.	
	Social media monitoring	Tools or services that track activity and metadata on social platforms.	
	Internet of things (IoT)	A network of physical devices connected to collect and exchange real-time data.	

DIGITAL TRANSFORMATION SOLUTIONS

2 TECHNOLOGIES | DATASTACK LAYER

Data Processing + Validation 1/2

USE CASE	TECHNOLOGY	DEFINITION	GENERATION
Template-based validation	Excel templates	Predefined spreadsheet formats used to validate data consistency and structure.	1G
Automated validation	API validation	Automated checking of data integrity through APIs.	2G
	Web form validation	Automatic checks to ensure correct data input in online forms.	
Task and process automation	Macros	Small programs that automate repetitive tasks in applications like Excel	3G
	Scripting (e.g., Python scripts, shell scripting)	Written scripts to automate tasks, such as data processing or file management.	
	Workflow automation tools (e.g., Zapier, Power Automate)	Platforms that automate workflows across multiple applications and services.	
	ETL and distributed processing tools (e.g., Apache Kafka, Hadoop, AWS Kinesis)	Tools for extracting, transforming, and loading (ETL) data at scale, often used in big data systems.	
	Robotic Process Automation (RPA) (e.g., UiPath, Automation Anywhere)	Software robots that record and replay human actions to automate structured business processes.	
Advanced text processing	NLP: Large Language Models (LLMs)	AI models that understand and generate human-like text based on natural language input.	4G
	NLP: Sentiment analysis	Technique to detect and interpret emotional tone in text data.	
	NLP: Topic modeling	Identifies topics present in a collection of documents.	
	NLP: Machine reading	Extracts and understands information from text to answer questions or summarize content.	
	NLP: Named Entity Recognition (NER)	Detects and classifies proper nouns (e.g., names of people, places, organizations) in text.	
	Other natural language processing (NLP)	Additional techniques like named entity recognition, language detection, and summarization.	

2 TECHNOLOGIES | DATASTACK LAYER

Data Processing + Validation 2/2

USE CASE	TECHNOLOGY	DEFINITION	GENERATION
Advanced image processing (e.g., CV, OCR)	CV: Optical character recognition (OCR)	Converts printed or handwritten text in images into machine-readable text.	4G
	CV: Biometrics	Uses facial, fingerprint, iris, or other physical feature to identify individuals.	
	Other computer vision (CV)	Visual analysis tasks like object detection, image classification, and scene recognition.	
Advanced document processing (e.g., PDF extraction)	PDF extraction	Extracts text, tables, and images from PDF files for analysis or transformation.	4G
Big data processing tools	Pyspark	A Python API for Apache Spark used to process large datasets in a distributed computing environment.	4G
	Cuda	A parallel computing platform and API model by NVIDIA for using GPUs in processing.	
	GPUs	Graphics processing units used to accelerate data processing, especially in AI and big data.	
	ELT Tools (e.g. Apache Kafka, Hadoop)	Tools that extract, load, and then transform data, commonly used in real-time and big data pipelines.	
	Quantum computing	Advanced computing methods used for secure data processing and future-proof cryptographic storage.	

DIGITAL TRANSFORMATION SOLUTIONS

2 TECHNOLOGIES | DATASTACK LAYER

Data storage

USE CASE	TECHNOLOGY	DEFINITION	GENERATION
"Digital file-based storage"	Shared network server folders and digital media	Storage of digital files on network drives or physical media accessible by multiple users.	1G
Databases	Relational database (e.g., MySQL, PostgreSQL, SQL Server)	Structured databases using tables and SQL for querying and data management.	2G
	Document-based and NoSQL database (e.g., MongoDB)	Flexible, schema-less databases ideal for storing unstructured or semi-structured data.	
	Graph-based database (e.g., neo4j)	Databases designed to represent and analyze relationships between data points.	
	Distributed ledger technology (e.g., blockchain)	A decentralized database that ensures secure, transparent, and immutable record-keeping.	
	Cloud-based file storage (e.g., AWS S3, GCS)	Scalable cloud platforms for storing and accessing files and objects over the internet.	
	Other database	Any other form of database not covered above, such as object-oriented or time-series databases.	
Consolidated storage platforms	Data warehouse: Snowflake	A cloud-native data warehousing platform known for scalability and separation of compute/storage.	3G
	Data warehouse: Elastic Stack	A suite (e.g., Elasticsearch, Logstash, Kibana) for storing, searching, and analyzing large datasets.	
	Data warehouse: IBM DB2	IBM's enterprise-grade RDBMS used for transactional and analytical workloads.	
	Data warehouse: Amazon Redshift	AWS's scalable cloud data warehouse designed for OLAP and real-time analytics.	
	Data warehouse: Google BigQuery	Google's serverless data warehouse for fast SQL-based big data analytics.	
	Other data warehouse	Any additional platforms used for large-scale structured data storage and analytics.	
Advanced storage systems	Data Lakes	Centralized repositories that allow storage of structured and unstructured data at any scale.	4G
	Other advanced storage systems	Includes hybrid storage solutions and novel data architectures for scalability and speed.	

2 TECHNOLOGIES | DATASTACK LAYER

Data analytica

USE CASE	TECHNOLOGY	DEFINITION	GENERATION
"Statistical summaries"	Static key performance indicators (KPIs)	Predefined metrics used to monitor performance over time, usually without real-time updates.	1G
Descriptive/Diagnostic analytics tools	Static analytical report	Non-interactive reports showing summaries and trends in historical data.	2G
	Dashboard (e.g., Tableau, Power BI)	Interactive visual interfaces for monitoring and analyzing key metrics and data insights.	
Predictive Analytics (e.g., ML)	Machine Learning (ML) (e.g., regression models, decision trees, deep learning)	Algorithms that learn from data to make predictions or classifications.	3G
	Recommendation engines	ML systems that suggest items or content based on user behavior or preferences.	
	Graph and network analytics	Analytical techniques for exploring relationships and connections within complex networks.	
	Risk modeling and stress testing	Predictive models that assess the impact of adverse scenarios on systems or businesses.	
	Time series forecasting (e.g., ARIMA, LSTM)	Techniques for predicting future values based on past time-dependent data.	
	Other predictive modelling techniques	Includes ensemble models, deep learning, or hybrid approaches not explicitly listed.	
Prescriptive Analytics	Optimization tools (e.g., linear programming, constraint programming)	Mathematical techniques for finding the most efficient or cost-effective solution under constraints.	4G
	Simulation tools	Systems that mimic real-world processes to test outcomes and improve decisions.	
	Early warning systems	Tools that detect signs of emerging risks or anomalies to trigger timely interventions.	
	Decision support	Systems that aid decision-making by evaluating scenarios, often combining predictive and prescriptive methods.	

2 TECHNOLOGIES | DATASTACK LAYER

Data products

USE CASE	TECHNOLOGY	DEFINITION	GENERATION
"Digital file-based report generation"	Templated reporting mechanisms (e.g., Excel charts, Word documents)	Reports using predefined templates to standardize outputs.	1G
Static Charts and Metrics	Key performance indicator (KPI) tracker	Tools for monitoring and displaying specific performance metrics over time.	2G
	Static time series charts	Non-interactive visualizations showing trends in data over time.	
Interactive visualizations	Geographic Information Systems (GIS)	Tools that visualize spatial or geographic data on maps for analysis.	3G
	Exploratory analysis	Interactive data tools allowing users to probe and visualize datasets to uncover patterns or anomalies.	
Advanced business intelligence tools (e.g., AI-driven)	Forecasting	Predicting future trends or values using statistical or AI methods.	4G
	Scenario modelling	Simulating different business or operational conditions to evaluate potential outcomes.	
	Natural language querying	Systems that allow users to query databases or analytics tools using everyday language.	
Generative AI (GenAI)	Image generation	AI-based creation of images from text prompts or other inputs (e.g., DALL·E).	4G
	Text summarization (e.g., GPT)	Using AI to condense long texts into concise summaries while preserving key information.	
	Generative Adversarial Networks (GAN)	Machine learning models that generate realistic synthetic content by training two competing networks.	
	Synthetic data generation	Creating artificial datasets that mimic real-world data for testing or training AI models.	
	Retrieval augmented generation (RAG) systems	Combines generative AI with retrieval systems to enhance responses using external knowledge.	

DIGITAL TRANSFORMATION SOLUTIONS

www.dtsolutions.io | info@dtsolutions.io

GOVSPACE