Financial InterGroup UK

Secretariat of the Basel Committee on Banking Supervision,
Bank for International Settlements,
CH-4002 Basel,
Switzerland

via email to: baselcommittee@bis.org

28 June 2013

To: The Basel Committee,

We welcome this opportunity to comment on the consultative paper issued by the Basel Committee on Banking Supervision (Committee) in March 2013 entitled 'Supervisory Framework for Measuring and Controlling Large Exposures' (LE Paper)[1].

Our interest in this subject matter is the consequence of our ongoing research into improved mechanisms and techniques for risk quantification and risk data aggregation. Our specific research has explored these areas from the following perspectives:

- 'Risk Accounting"... the convergence of accounting and risk management systems within a common enterprise exposure measurement framework[2]
- 'Global identification' for data aggregation (the Legal Entity identifier (LEI)[3] …standards and counterparty exposure aggregation capabilities
- 'Big Data' … intelligent semantic network for systemic risk analysis[4]

We collectively refer to these research initiatives, all of which have been translated into implementation modules, as 'risk adjusting the financial system'. Given the reasonable timeframe

[1] Supervisory Framework for Measuring and Controlling Large Exposures at http://www.bis.org/publ/bcbs246.pdf

[2] Grody AD, Hughes PJ, Fernandes KJ, Phillips O, and Toms JS, '*Risk Accounting: An Accounting Based Approach to Measuring Enterprise Risk and Risk Appetite'* (October 20, 2012). Available at SSRN: http://ssrn.com/abstract=2165034, and Hughes P, Grody AD, Toms JS, 2010, *'Risk accounting - a next generation risk management system for financial institutions'*, The Capco Institute Journal of Financial Transformation, 29 (1): 43-56

[3] Grody AD, Hughes PJ, and Reininger D, *'Global Identification Standards for Counterparties and Other Financial Market Participants'* (March 6, 2012), Journal of Risk Management in Financial Institutions - Special Issue on Counterparty Risk, Vol. 5, No. 2. Available at SSRN: http://ssrn.com/abstract=2016874

[4] FIORD submission, accepted for presentation, *Collaborative Business Processes and Service Architectures,* PRO-VE'13 - 14th IFIP Working Conference on Virtual Enterprises at http://www.pro-ve.org/

for implementing the recommendations found in the LE paper (2019) we believe our proposals are implementable within this timeframe.

Sincerely,
Peter J. Hughes
Managing Director
Financial InterGroup (UK) Ltd

Allan D. Grody President: Financial InterGroup Holdings Ltd Former Adjunct Professor, Stern Graduate School of Business, New York University 169 East 69th Street - 18th floor New York, New York 10021 Phone: +1 212 585 0409 Email: agrody@FinancialInterGroup.com Financial InterGroup	**J. Steven Toms** Professor of Accounting Leeds University Business School University of Leeds Leeds LS2 9JT Phone: +44 (0) 113 343 4456 Email: j.s.toms@leeds.ac.uk UNIVERSITY OF LEEDS
Kiran J. Fernandes Professor of Operations Management Durham University Business School Durham University Durham DH7 9RH Phone: +44 (0) 191 334 5512 Email: k.j.fernandes@durham.ac.uk Durham University	**Peter J. Hughes** Visiting Research Fellow The York Management School University of York Freboys Lane York YO10 5GD Phone: +44 (0) 7766 916541 Email: peter.hughes@york.ac.uk THE UNIVERSITY of York

Response to the Consultative Paper - Supervisory Framework for Measuring and Controlling Large Exposures

Fernandes, K.J., Grody, A.D., Hughes, P. J., Toms, J.S.

28th June 2013

Introduction

We share the Committee's concern of avoiding undue complexity when formulating its supervisory frameworks and associated rules. The fact remains, however, that bank regulation is already excessively complex and, in many circumstances requires updating rather than incremental change. Indeed, we would say it needs a significant rethink. It is to this end that our research has been focused for some years and provides the basis of the comments contained in this letter.

The need for a rethink finds some substantiation in the LE Paper itself. Whereas it is intended, as far as possible, to follow the existing relevant frameworks such as the risk-based capital requirements as defined by the Basel II framework, the LE Paper seeks simpler solutions. For example, the Committee explains that for the determination of large exposure reporting if a simpler approach already exists and there is a case for it, it is chosen "for example, to avoid model risk".[5]

The Current State of Bank Regulation and Accounting

There is much written and spoken on the issue of complex and flawed regulatory regimes. For example, Haldane (2012)[6] commented that due to escalating complexity "the Tower of Basel is at risk of over-fitting – and over-balancing" concluding that simpler, more judgment-based approaches to regulation should be considered. He was particularly critical of the role risk models play in modern bank supervision with reference to "startling degrees of complexity and an over-reliance on probably unreliable models.... With thousands of parameters calibrated from short samples, these models are unlikely to be robust for many decades, perhaps centuries to come. It is close to impossible to tell whether results from them are prudent."

The Committee has also voiced criticism of its own risk-based capital regime. In its recent review of trading book capital requirements[7] reference was made to "material weaknesses" with comments such as, "flaws in the overall design of the framework" and "both the models-based and the standardized approaches proved wanting". Most significantly, the Committee observed that the prevailing regulatory capital adequacy regime constituted a "provision of incentives for banks to take on tail risk" which is contrary to precisely what a regulatory capital regime is intended to prevent.

[5] LE Paper - Paragraph 42

[6] '*The dog and the Frisbee'*, Andrew G Haldane and Vasileios Madouros, presented at the Federal Reserve Bank of Kansas City's 36th economic policy symposium, "The Changing Policy Landscape", Jackson Hole, Wyoming, August 2012

[7] '*Fundamental Review of the Trading Book'*, consultation by the Basel Committee on Banking Supervision, May 2012

Rowe (2010)[8] aptly described the adverse role complexity plays in modern bank regulation, "... the painful financial and economic upheaval of the past three years (financial crisis) can be traced to unbridled complexity outrunning the ability of both public and private organisations to control it effectively... complexity might have worthy primary goals but breeds little understood dangers... I have reluctantly come to the conclusion that regulatory capital rules fall into this latter category"

We also recognize that the accounting profession has not addressed the question of accounting for risk given that its standards[9] are oriented towards accounting for fair values. The result is accounting processes that are designed to provide a static measure of financial condition. This is of little value to regulators who must concern themselves with the true economic condition of financial institutions which requires consideration of the probability and severity of future losses that are likely to occur in extreme but plausible operating and macroeconomic scenarios.

Adding Incrementally to an Excessively Complex Basel II Foundation

It would appear from the LE Paper, in response to the circumstances described above, that the Committee is introducing regulatory reporting requirements that are designed to limit the negative effects of its own capital adequacy regime defined in Basel II. Indeed, the LE Paper states that the "large exposures framework is constructed to serve as a backstop and complement to risk-based capital standards".[10] Such a regulatory device is not new. For example, the leverage ratio introduced in Basel III is also intended to function as a Basel II backstop through the provision of "safeguards against model risk and measurement error by supplementing the risk-based measure with a simple, transparent, independent measure of risk".[11]

The practice of compensating for the flaws inherent in the existing risk-based capital regime by supplementing it with additional, albeit simpler requirements can only add further complexity to an already overly complex regulatory framework. Within the Committee's rules, regulated financial institutions must contend with multiple methods of calculating 'exposure' for the same financial instruments whereby: the foundation (Basel II) used for capital adequacy purposes is widely viewed as overly complex and flawed; a simpler exposure measurement method may be chosen for large exposure reporting; and accounting 'fair value' definitions are used for the application of the Basel III leverage ratio. We also observe that regulators in certain jurisdictions have proposed modifications to the application of fair value accounting standards (introduction of 'prudent valuation') when calculating the amount of a financial institution's own funds.[12]

In our judgment it is misguided to believe that an overly complex and flawed regulatory regime can be improved and made more secure by adding incrementally to it particularly where additional rules are intended to limit the negative or unintended consequences of earlier rules.

---

[8] '*Regulators Double Down'*, David Rowe, Risk Magazine, December 2010, accessible at http://www.risk.net/risk-magazine/opinion/1895760/regulators-double

[9] For example, International Financial Reporting Standards (IFRS)

[10] LE Paper - Paragraph 14

[11] *'Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems'*, Bank for International Settlements, June 2011

[12] For example, European Banking Authority, *'Discussion Paper: Relating to Draft Regulatory Technical Standards on prudent valuation under Article 100 of the draft Capital Requirements Regulation (CRR)'*, November 2012

It cannot be acceptable to regulated financial institutions that they must divert so much of their resources in the maintenance of multiple versions of the same information so that they are positioned to respond to inconsistent regulatory rules and accounting standards. It cannot be acceptable to users of the global financial system and those that invest in it to be presented with audited financial statements based on accounting standards that do not give recognition to all the risks inherent in the transactions financial institutions accept for processing. It cannot be acceptable to boards and senior executives of financial institutions to be presented with financial reports that reflect diverse versions of economic condition and capital driven by accountants' and risk managers' different perspectives of what constitutes exposure and how it should be reported. It cannot be acceptable to regulators that they are unable to observe the build-up of exposure to risk in the global financial system on a complete, consistent and timely basis.

Reengineering the Global Financial System

There comes a point when a system achieves a degree of complexity, permeated by a myriad of internal interdependencies, that it must be declared as no longer fit-for-purpose; a point when its operators can no longer reliably anticipate the consequences of system modifications that, from time-to-time, they are required to make. The dilemma is that any modification to the system can potentially trigger, in the best case, unintended consequences and, in the worst case, its total breakdown. We believe that the financial crisis provides indication that the global financial system has already achieved the latter condition. In such circumstances, the only option is to reengineer the system over time while providing a parallel path to support regulatory oversight until the reengineered state is achieved.

What will such a reengineered system look like? If it is to provide regulators with the framework through which effective supervisory oversight can be exercised then it will need to have the following features:

- A simplified and replicable method of calculating exposure to risk that can be universally applied to sources of transactions that are reconcilable to accounting records
- Global identification standards for legal entities, products and financial events to facilitate the aggregation and comparison of risk exposure data within and between financial institutions and across the industry
- A 'Big Data' framework that is able to provide regulators and others with complete and accurate real-time information relating to the global financial system

It is precisely these areas that have been the object of more than a decade's research by Financial InterGroup in collaboration with York, Leeds and Durham universities and others. Our aim was to design a blueprint for a reengineered global regulatory framework with a view to 'risk adjusting the financial system'.

In so doing due consideration was given to a most recent and relevant paper issued by the Committee[13] that sets out new requirements due for implementation in 2016 including:

[13] Basel Committee on Banking Supervision, '*Principles for Effective Risk Data Aggregation and Risk Reporting',* January 2013

1. Controls surrounding risk data should be as robust as those applicable to accounting data
2. Supervisors expect banks to consider accuracy requirements analogous to accounting materiality
3. Risk data should be reconciled with bank's sources, including accounting data where appropriate, to ensure that the risk data is accurate
4. The term 'risk data aggregation' means defining, gathering and processing risk data according to the bank's risk reporting requirements to enable the bank to measure its performance against its risk tolerance/appetite

Our proposed framework that addresses these requirements is termed 'Risk Accounting'; an overview is provided in Appendix 1.

The Global Legal Entity Identifier System (GLEIS) Initiative

We have also actively participated in, and contributed to the Global Legal Entity Identifier System (GLEIS) initiative that was mandated by the G20 and is currently being developed and implemented under the oversight of the Financial Stability Board; an overview is provided in Appendix 2.

This system has at its root the same interest in aggregating control groups of counterparties as is described in the LE paper. We believe the mechanism proposed by us to the Financial Stability Board and now its implementation arm, the Regulatory Oversight Committee, is the foundation for aggregating counterparty risk data for large exposure reporting.

Large exposures of aggregated parent/child counterparties requires the identity of an ultimate controlling business entity to be associated with each counterparty, subsidiary or other financial transactors in the hierarchy of business entity relationships controlled by the ultimate parent. Each such hierarchical tree needs a mechanism to easily identify and then aggregate associated risk data.

We have proposed that those tree structures of ownership are to be defined using a unique coding convention for legal entity identification and the account consolidation rules found in GAAP and IFRS accounting. Where interpretations of those rules or judgments about the rules are required professional accountants will be called upon to "certify" such structures. They will work from original source documents such as articles of incorporation and the historical record found in audit working papers.

Similarly, hierarchical counterparties under the control of a control entity as with SPEs or SIVs will be interpreted by appropriate professionals using offering documents, trust agreements, initiating contracts and the like.

Where connected counterparties outside the traditional parent/child/control entity relationship pose a single risk, such as financial entities subject to the same or similar variation margin calls, a group of credit protection providers, a common bank risk regime requiring specific collateral instruments, fund families and other collective investment vehicles, etc. we have proposed a definition of such risk regimes or economic interdependencies be part of the LEI stored reference data elements. This will enable data aggregation across this dimension of interconnectedness.

With such a legal entity identification system in place for hierarchical construction of counterparties, the comparison of control entities' and control groups' risk exposures is facilitated. Concentration of

risk across business silo levels, third parties, and single names is aggregatable. Comparisons to established limits or triggers can, thus, be accomplished. What those triggers or limits are we leave to others to opine on.

Central Counterparties (CCPs)

Central counterparties (CCPs) pose another form of interrelated risks, the risk of multiple CCPs being economically interdependent and the risk of multiple counterparties, external to the CCP, being economically interrelated, causing further interdependencies at the CCP level. The use of multiple CCPs, potentially causing higher collateral requirements and affecting the bilateral netting benefit of counterparties using single or few dealers can be offset. Net overall tail risk can be computed for each counterparty. This can be accomplished by aggregating the netted positions of each counterparty in each CCP. Recall that counterparties in the LEI system are uniquely and universally identified in each CCP. The net risk of each counterparty's position is used to compute a capital increment or decrement for the introducing CCP's clearing member bank that, in turn, has a call on capital, in the form of margin from the counterparty itself.

CCPs pose still another risk, that of being 'too-big-to-fail'. However, before a government led bailout, the last resort of any collapsing financial system, it could well be that a government led bailout fund, contingently funded by private capital, perhaps through drawdown commitments could be applied as the first tranche of such a bailout fund. With the experience of the US's Troubled Asset Relief Programme (TARP) funding and the ROI that those funds earned, it should be an attractive proposition for capital managers. Such capital sources, in the form of hedge funds and private equity investors, endowments and pension funds, family offices and sovereign funds, may find an asset class that does not require actual funds to be locked up attractive, but rather sells a call option to central counterparties, earns a return, and is prepared to lend money at agreed to rates when called upon. This is the equivalent of catastrophic insurance, but funded not by the insurance industry, but by private pools of capital.

An Intelligent Semantic Network for Systemic Risk Analysis

Finally, the key elements of an intelligent semantic real-time 'Big Data' financial network were presented by Financial InterGroup and others to the Securities Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the US Treasury's Office of Financial Research. This was in response to these three agencies' separate solicitations of interest in a global identification system for immediate use in swaps regulation and data reporting. Its broader aim was to assist in aggregating data for systemic risk analysis.

Most recently the evolving first stage of this global identification system, the Legal Entity Identification (LEI) network was proposed to the European Union (EU) as the backbone of an intelligent semantic network for systemic risk analysis. The network is referred to as the Financial Industry Ontologies for Risk and Regulation Data (FIORD); an overview is provided in Appendix 3. The proposal was submitted under the EU's Seventh Framework Program (FP7) for research this spring by a consortium of European Universities, financial institutions and technology companies. Its aim is to provide novel algorithms, software infrastructures and methodologies for real-time interaction, visualization, analytics and decision support applications over extremely large volumes of data (both

structured and unstructured) that comprise the global financial system. Allan Grody of Financial InterGroup is Chairman of the FIORD Advisory Board.

Summary

We respectfully submit our comments in this letter and in the appendices that follow with the aim to inform the Committee that the reengineering of the regulatory framework, as we propose, is not only necessary and viable, but most importantly implementable within the Committee's proposed stages for risk data aggregation set for 2016 and large exposure reporting set for 2019.

We note that we are engaged in all aspects of these implementations and look to the Committee to provide its bully pulpit to advocate for our cause which should be its own. In this regard we believe our approach meets the current demand for simplified approaches to the regulation of financial institutions. We hope we have demonstrated that this is eminently achievable through mechanisms and techniques that: align risk management with accounting standards and systems; deploy technological advancements to aggregate vast quantities of risk data for computer aided regulatory oversight of the financial system; and makes use of a universal identification system of financial market participants and the financial instruments and contracts they own, trade and process to provide a consistent and uniform means to understand large exposures of both singular and interconnected counterparties.

Appendix 1

Risk Accounting - Overview

Risk Accounting is a next generation Enterprise Risk Management system[14]. It addresses the weaknesses and limitations in banks' risk management and accounting systems that failed to provide forewarning of life-threatening accumulations of exposure to risk that formed the backdrop to the financial crisis.

Risk Accounting introduces a simple, consistent and auditable method of measuring and reporting enterprise risks as an extension of management accounting. It comprises three categories of tables and templates that assign standardised risk-weights to individual transactions according to:

1. The risk characteristics of the relevant products
2. The amounts accepted for processing in accordance with accounting records
3. The risk mitigation effectiveness of the operating environment that handles them

The risk-weights tagged to each transaction are used in a calculation of its exposure to risk. In this way, Risk Accounting accounts for the risk exposures inherent in transactions and produces risk reports that can be aggregated by risk type (credit, market, liquidity and operational) and by organisation, geography, product and customer.

Risk Accounting's tables and templates are built from the ground up incorporating the expert knowledge of line and risk management which becomes embedded in the very fabric of the risk measurement method. The result is risk metrics that are both credible and actionable allowing a risk culture to naturally evolve with continual risk mitigation as the outcome.

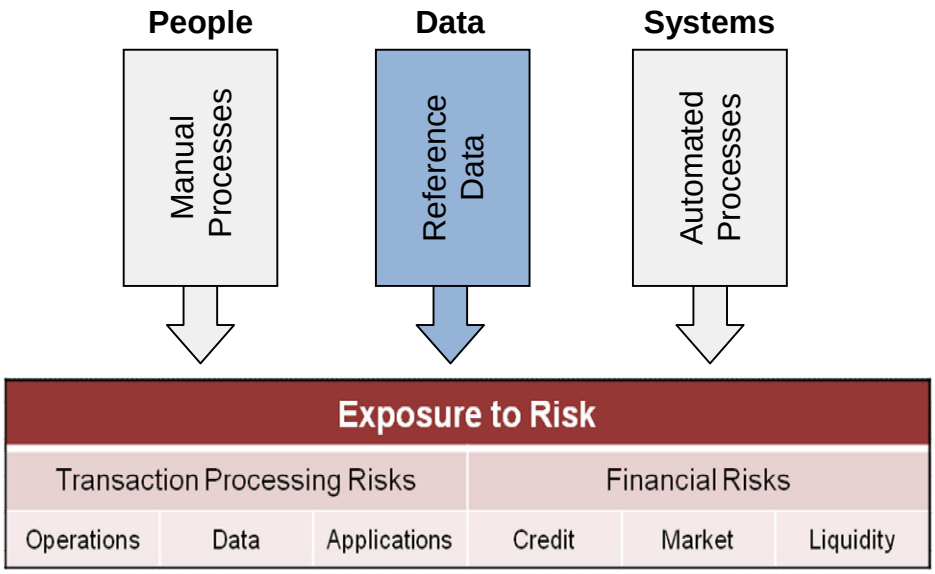
Risk Accounting's standard unit of risk measurement – the Risk Unit (RU) – blends quantitative and qualitative risk elements into a single additive metric that can be used in the setting and monitoring of risk appetite.

Real-time management dashboards facilitate the management of risks by exception – primarily risk appetite excesses – enabling analysis of the causes by drilling to the relevant products and related processes.

How Exposure to Risk is Created

An operating environment can be deconstructed into the simple model shown below represented by three key operational pillars – people, data, and systems. If the interaction of the three operational pillars (manual process, automated process, and data) is flawless a theoretical risk-free operating environment is the result. Thus, the benchmark for a risk-free operating environment can be represented as 100 per cent straight-through-processing (STP) with totally reliable and secure information technology and flawless data.

[14] See footnote 2



The Three Pillars of an Operating Environment

This benchmark also represents a transaction processing environment that is operating at or close to optimal efficiency. Consequently, the correlation between risk mitigation effectiveness and operating efficiency is either '1' or close to '1'.

It follows that exposure to risk, and the loss of operating efficiency, are the consequence of the failed and/or insecure interaction of manual processes and automated processes with data relative to the processing of transactions and the management of financial risks. The risk metrics produced by Risk Accounting are aligned to this dynamic.

The Risk Unit (RU) – Three Core Metrics

The risk quantification method involves the production of three core metrics using the new common unit of exposure measurement unique to Risk Accounting... the 'Risk Unit' (RU):

Inherent Risk – is the risk-weighted size of a transaction expressed in RUs that represents the transaction's maximum potential for loss

Risk Mitigation Index (RMI) – is a dynamic measure on a scale of 1 to 100, where 100 is best practice, that represents, in percentage terms, the portion of maximum potential loss that is mitigated through the effective management and control of the firm's operating environment

Residual Risk – is expressed in RUs and represents the probability of loss being the portion of Inherent Risk not covered by effective risk mitigation as represented by the RMI

The above core metrics are calculated at the transaction level relative to the risk types that are triggered by a transaction and can be one or a combination of operational, credit, market and liquidity risks. The resulting metrics can be aggregated by, for example, organization, product, customer, geography and risk type.

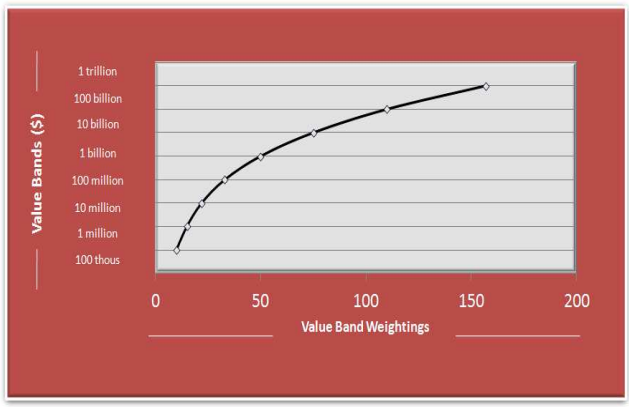
Preventing Unexpected Losses

The amount of risk inherent in a transaction accepted for processing relates to its potential to cause unexpected losses. An unexpected loss can be prevented through a firm's effective monitoring and management of the associated risks. This is precisely what Risk Accounting is designed to facilitate.

An unexpected loss occurs in circumstances where a firm's management believes its risk management processes are effective but, in reality, they are not due to failures either in their design or application. It follows that an unexpected loss cannot result from a firm intentionally taking on a risk for a projected return if the decision to accept such risk is a consequence of the application of effective risk management processes represented by a high Risk Mitigation Index (RMI) and within approved risk appetite parameters.

The Value Table

The Value Table comprises value bands and associated risk-weights (Value Band Weightings). The resulting logarithmic curve shown in the table below depicts the relationship between transaction values and risk, i.e. the marginal increase in risk reduces as transaction (processing) values increase. This is due to the natural increase in the sophistication of processing that occurs when transaction throughput increases due, primarily, to enhanced automation.



The Value Table

These value bands adjust dynamically to the product volumes and values being processed and are scaled accordingly.

Financial Risks and Exposure Uncertainty Factors (EUFs)

Risk Accounting introduces a new concept in risk quantification… the Exposure Uncertainty Factor (EUF). The EUF assumes that there is a positive correlation between a product's potential to cause unexpected losses and the degree of exposure uncertainty that exists, for example, upon the assumed occurrence of a credit default (credit risk) or if a trading position were to be unwound on any given day (market risk).

Research has demonstrated that the EUF offers a more reliable basis on which to calculate forward looking exposures to risk than the more backward looking risk models – such as Value-at-Risk (VaR) – that rely on historic loss data to predict the probability and severity of future unexpected losses.

For example, exposure uncertainty relative to credit risk is a function of a credit's underlying collateral by reference to its value retention properties and degree of anticipated difficulty in arriving at a liquidation price upon disposal.

Credit Type	Form of Security / Type of Instrument	EUF
Commercial	Casual Overdraft	2
Commercial	Credit Card	2
Commercial	Unsecured	2
Commercial	Cash	4
Commercial	Cash Like Instruments (Margins, Liquid AAA Collateral)	5
Commercial	Trade Receivables	8
Commercial	Inventory	12
Commercial	Equipment	12
Commercial	Instruments Subject to Mark-to-Market, Mark-to-Model	12
Commercial	Autos	12
Commercial	Personal Guarantee	14
Commercial	Project Financing	16
Commercial	Commercial Real Estate	18
Counterparty	Forward Foreign Exchange	4
Counterparty	Interest Rate Swaps	8
Counterparty	Options	8
Counterparty	Credit Default Swaps	14
Counterparty	Collateralized Debt Obligations and Asset Backed Securities	18
Retail	Casual Overdraft	2
Retail	Credit Card	2
Retail	Unsecured	2
Retail	Autos	12
Retail	Personal Guarantee	14
Retail	Residential Property	16

Credit Risk – Exposure Uncertainty Factors (EUFs)

Credits secured by collateral with a high EUF carry correspondingly high inherent credit risk. This is due to their exposing a firm to greater probability of unexpected losses because credits that are deemed secured may become partially or wholly unsecured due to an inherent susceptibility to changes in the value and/or availability of the collateral and/or difficulty in liquidating the assets.

Conversely, an unsecured loan has a low EUF and a correspondingly low inherent credit risk as the true exposure at default can be readily determined. A table of sample EUFs for credit risk is shown above.

Transaction Processing Risks

Upon their acceptance for processing, transactions follow a predetermined path through the operating environment. This path is represented by operations units that perform certain activities relative to the transactions, for example, data capture, release of values (payments), reconciliation, independent checking, valuation (mark-to-market), imaging, placing/removing into/from safekeeping and many more.

Operational activities have varying degrees of inherent risk. For example, an activity that releases values to third parties is inherently riskier than imaging a document. The criteria applied in determining the degree of inherent risk is 'loss immediacy'. If an operational process is faulty the occurrence of a loss is more likely if the loss is immediate upon the faulty activity being executed.

Research to date has identified 34 such operational activity types that have been catalogued and a relative risk weighting assigned.

Activity Type	Activity Description and Examples	Weighting
General Administration	General administration • Imaging • Filing • General support	1
Nostro Investigation	Investigation, aging and escalation of unmatched items	6
Payments / Settlements	Release value items (including standard settlement instruction and standing order / direct debit maintenance) to: • Guaranteed counterparties • Intercompany and intra-company • Guaranteed settlement (e.g. central exchanges / Continuous Link Settlement) • Delivery versus payment agreements	2
	Release value items (including standard settlement instruction and standing order / direct debit maintenance) to: • Financial market counterparties • Banks and other financial institutions	5
	Release value items (including standard settlement instruction and standing order / direct debit maintenance) to: • Other parties • Non-financial market counterparties • Third parties	10

Operational Activity Catalogue (Extract)

An extract from the operational activity catalogue is shown above. Risk Accounting uses these risk weights in the calculation of inherent risk RUs relative to individual transactions.

Best Practice Scoring Templates (BPSTs)

BPSTs are used to calculate the Risk Mitigation Index (RMI) which is a measure of the risk mitigation effectiveness of the operating environment.

Credit Assessment & Approval	
Relates to assessment and approval processes applied in credit-granting decisions	
Best Practice Score = 100 Points	
Best Practice Statements	**Deductible Points**
1. The organisation's approved credit risk management procedures set out the credit-granting processes and documentation standards that must be complied with when assessing and approving credits	100
2. The organisation's approved credit risk policies set out credit-granting criteria encompassing the individuals and organisations that are eligible for credit (exclusive and inclusive), the terms and conditions and the amounts and types of credit that can be transacted. This is followed for every credit approval	100
3. While assessing credit proposals for an obligor, complete and accurate aggregate exposures of related parties are available for evaluating the overall risks including concentration risks	70
4. Specialist credit analysts, who are assigned to a business line but report independently of the management of business origination personnel (sales), analyze and approve credits and have the authority to amend the internal credit risk ratings (downgrade or upgrade) assigned by business origination personnel (sales)	60
5. The organisation relies on its own independent credit assessment and analysis of each obligor even if third party credit assessments and/or ratings are available	50
6. Credits outside of business 'strike zone' require approval by an independent credit review function	40
7. Each obligor is assigned an internal credit risk rating by personnel who are sufficiently knowledgeable of the obligor's circumstances to reliably conclude on the reputation and creditworthiness and are suitably expert in credit analysis and assessment.	40
8. Personnel who have been assigned lending authority can approve credits up to predetermined limits based on a combination of pre-defined parameters including internal credit risk rating and the amount of credit being granted	40
9. Override of system generated internal risk ratings is done only by credit personnel with authorities for overrides. Reasons for override are documented as a part of the credit approval	40
10.In addition to credit approvals, for credits where the *Risk Adjusted Return on Capital (RAROC)* is lower than the hurdle rate as per pricing policy, separate pricing approvals are required by personnel independent of the business origination personnel (sales)	20
11. Organisation has standardized templates for credit analysis (including financial analysis) to minimize variance in credit assessment process	20
12. As a part of credit approval process all obligors are subject to Know Your Customer (KYC) background checks as required by regulations applicable to the organization	20
13. Credit approval workflow automatically ensures that the proposal is routed to the correct level of credit personnel for approval. Exceptions are immediately triggered for action	10

Sample Credit Risk Best Practice Scoring Template

A primary input to BPSTs are the 'effective principles' and 'sound practices' papers published from time-to-time by the Basel Committee on Banking Supervision.

BPSTs have been developed for each risk type and comprise generic and risk specific templates. For example:

- Generic BPSTs include People, Controls, Execution and Business Recovery

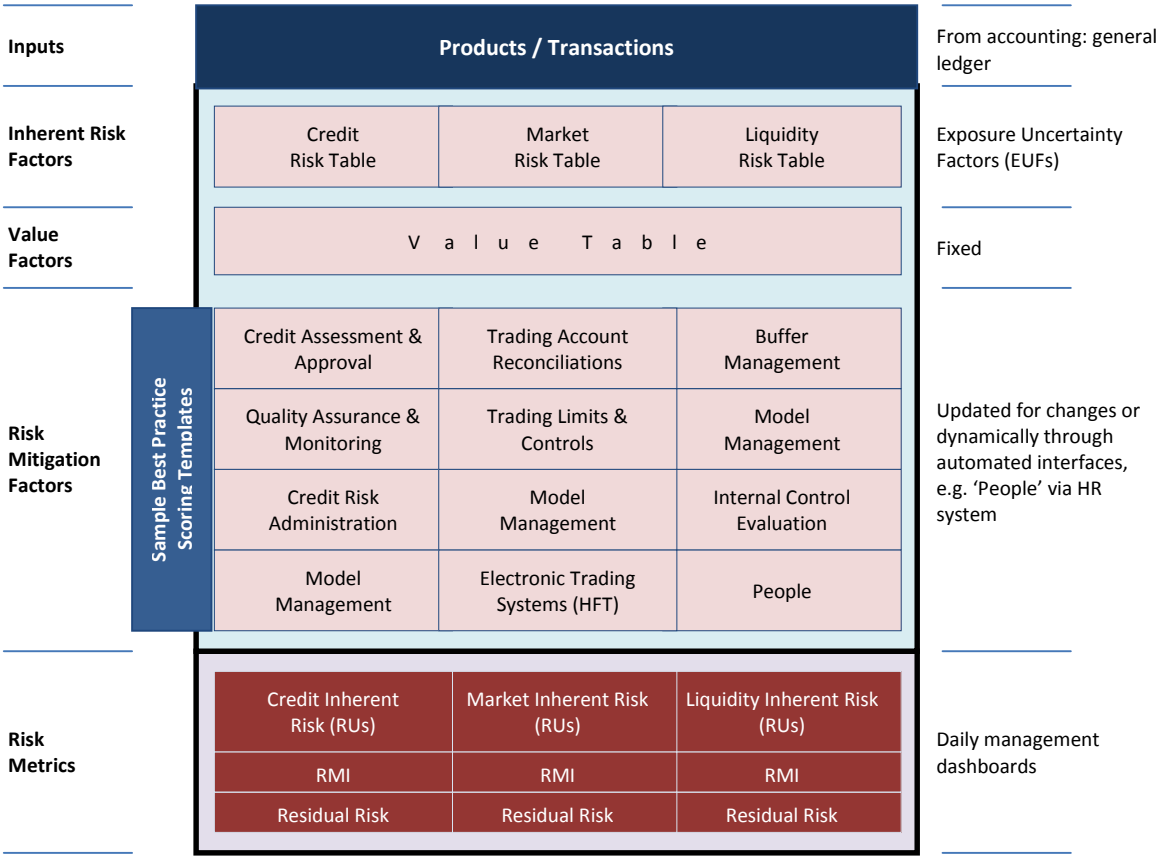
- Risk specific BPSTs include, for credit risk, Credit Assessment & Approval, Credit Quality Assurance & Monitoring, Credit Risk Administration and Credit Risk Model Management
- Operational (transaction processing) risk comprises Manual Processing (Operations), Automated Processing (IT) and Data Management.

Above is a sample BPST for Credit Assessment & Approval. The 'deductible points' represent the relative degree of reliance that management places on the respective best practice when designing and applying credit risk management processes.

In deriving a best practice score for 'Credit Assessment & Approval' relative to a product, scoring begins with the maximum '100' and for each best practice that is not complied with the respective 'deductible points' is deducted cumulatively from the maximum '100'. A resulting score can be zero but not less than zero.

Risk Accounting - Process Overview

The diagram below relative to financial risks (transaction processing risks are not shown) shows the flow of transaction data from the general ledger through the various tables and templates that comprise the Risk Accounting method and system.



Risk Accounting Process Flow – Financial Risks

Reporting

Risk accounting is designed to identify and quantify external exposures to risk from two perspectives:

1. The amount of new exposures to risk created during a particular day ('Daily New Exposures')
2. The amount of risk inherent in risk positions at a given point in time ('Risk Positions').

The transactions that comprise 'Daily New Exposures' and 'Risk Positions' are derived from, and are traceable to the firm's general ledger and its associated product sub-ledgers and applications thereby satisfying Basel requirements that risk data should be reconciled to accounting data[15].

The amount of 'Daily New Exposures' relative to credit risk is determined for each product by reference to the total amount of loans disbursed, guarantees approved, etc. Where credit risk is not the result of a loan disbursement, e.g. casual overdrafts, credit card outstandings etc., the net day-to-day increase in total outstandings of the respective portfolio is considered to be the new daily credit exposures.

For market risk 'Daily New Exposures' is the aggregate trades (buys and sells) and related hedges relative to each trading position on the principle that abnormally high trading volume is an indicator of higher risk and such activities should be reflected in management reports albeit adjusted by the applicable Exposure Uncertainty Factor (EUF) discussed above. Aggregate values are also applied to the products and related hedges that comprise a market risk 'Risk Position'. A high EUF is an indication of the probability that these products and associated hedges, while validly combined and netted in a single trading position, may not provide the intended risk management effect if liquidated in stress conditions.

Transaction size is another factor in the calculation of RUs inherent in credit and market risk as a transaction's size (value) and the amount of unexpected loss it can potentially create are positively correlated.

In the case of market risk and counterparty credit risk with respect to derivatives, Risk Accounting considers that the notional values are representative of transaction size as they provide the basis on which future cash flows, mark-to-market and mark-to-model calculations, collateral deposits and related gains and losses are determined. When calculating the exposure in RUs inherent in 'Risk Positions' for both credit and market risk, Risk Accounting uses fair values or market values in accordance with accounting principles as these more accurately reflect the outstanding amounts.

A Better Method for Regulators and Investors

The product risk report shown on the following page provides an example of an output of Risk Accounting relative to the inherent and residual risks of a financial product; in this case, a Collateralized Debt Obligation (CDO). The interpretation placed on this example is that the inherent risk (4,650 RUs) is representative of the maximum potential for loss inherent in the CDOs transacted on a particular day and the residual risk (2,166 RUs) is representative of the respective probability of loss.

[15] See footnote 13

Collateralized Debt Obligations (CDOs)	Inherent Risk (Risk Units)	Risk Mitigation Index (RMI)	Residual Risk (Risk Units)
Processing Risks			
Transaction Processing Risk			
Product & Service Pricing	1,350	63.5	493
Deal Structuring	1,350	55.2	605
Order Management	1,350	68.2	429
Pre-Trade Validation	1,350	62.3	509
Quote Management	1,350	73.4	359
Trade Execution & Capture	1,350	44.9	744
Cash Management	1,350	52.3	644
Trade Confirmation & Matching	1,350	60.0	540
Position Control & Amendments	1,350	60.2	537
Transaction Reporting	1,350	63.2	497
Credit Limit Monitoring	1,350	45.0	743
Trading Limit Monitoring	1,350	62.4	508
Trade Settlements	1,350	63.4	494
Nostro Reconcilement	1,350	72.8	367
Trading Account Reconciliations	1,350	66.7	450
G/L Proofs & Substantiation	1,350	73.3	360
Management Reporting	1,350	64.2	483
Regulatory & External Reporting	1,350	64.2	483
Control Totals	24,300	62.0	9,245
Transaction Processing Risk	**1,350**	**62.0**	**514**
Data Quality			
Client & Counterparty	1,350	79.2	281
Market Data	1,350	52.9	636
Products & Instruments	1,350	68.2	429
Corporate Events	1,350	43.3	765
Control Totals	5,400	60.9	2,111
Data Quality	**1,350**	**60.9**	**528**
Business Systems (IT) Risk			
Integrated Trading System	1,350	78.9	285
Funds Transfer System	1,350	65.4	467
Global Nostros System	1,350	65.0	473
Global Ledger System	1,350	82.3	239
Funding & Liquidity System	1,350	69.4	413
Control Totals	6,750	72.2	1,877
Business Systems (IT) Risk	**1,350**	**72.2**	**375**
Control Totals	36,450	63.7	13,233
Total Processing Risks	**1,350**	**63.7**	**490**
Financial Risks			
Credit Risk Management	1,350	52.0	648
Market Risk Management	1,350	43.9	758
Liquidity Risk Management	600	55.0	270
Total Financial Risks	**3,300**	**49.2**	**1,676**
Total Product Risks	**4,650**	**53.4**	**2,166**

Sample Risk Accounting Report – Product Risk

Over time, Risk Accounting outputs will be correlated with expected and actual losses thereby imparting a monetary value to the RU. In the interim, benchmarking RUs across financial institutions that are adapting to the Risk Accounting method will provide relative standing of the RU's value to improving best practices and thereby mitigate risks.

Inasmuch as the Risk Accounting method quantifies inherent and residual risk in RUs relative to each product transacted by a financial firm, it follows that such information can be validly applied in the calibration of regulatory capital requirements. The expectation is for the RU metric, over time, to assume a statistically derived monetary value considering that the RU incorporates all of the principal risk types (credit, market, operational and liquidity).

For this potential to be realized it is acknowledged that the tables and templates that constitute the Risk Accounting method and system will need to be standardized across the industry, not unlike the prescriptive accounting standards disseminated as International Financial Reporting Standards (IFRS) that are designed to ensure, amongst other aspects, the comparability of firms' audited financial statements.

The benefits are, however, potentially significant for regulators as capital requirements based on RUs will be the result of explicit measurements of exposure to risk following auditable processes. Investors and other stakeholders will similarly derive benefit as they will be able to directly compare the level of risk accepted by a firm both absolutely and in comparison to others.

Appendix 2

The Global Legal Entity Identifier System (GLEIS)[16]

Financial service industry regulators are focused on observing systemic risk across highly complex interconnected global financial institutions. While these systemically important financial institutions continue to improve their enterprise risk management systems, regulators are now intent on adding new tools and techniques to analyze the risk exposures that arise across these firms. Many attempts are underway to understand how to aggregate risk within and across financial institutions and provide for transparency of financial transactions and risk exposures. It is understood that without an ability to view the underlying positions and cash flows, valued in standard ways and aggregated by counterparty through common identifiers, neither risk triggers nor risk exposures can be observed nor can systemic threats be detected.

It has been accepted by regulators that the first pillar of global financial reform is a standard for identifying the same financial market participant to each regulator in the same way. Getting agreement on a globally unique and standardized legal entity identifier (the LEI) is the first step.

Industry members and sovereign regulators, newly empowered through the G20's Financial Stability Board (FSB) are engaged in developing a global identification system for such purpose. Our research paper[17] reviews the origins of systemic risk in the financial industry and its related data issues and how standard identification of financial market participants and the products they trade connects to regulators' and financial institutions' ability to analyze systemic risk. It discusses proposals offered for a global identification system and approaches taken in other industries and economic sectors.

We have proposed a government and industry partnership in which governance is shared and operating elements of the global identification system are compartmentalized for control, security and confidentiality purposes. Our paper previews a global standards convention along with its operational and technical implementation. The standard LEI coding convention proposed is a unique, unambiguous and universal character set constructed around a two part apportionment and assignment process between regulators and financial market participants. It is shown that this two part construction is essential to accommodate requirements of sovereignty, control and confidentiality put forward in more recent regulatory requirements. It is also shown that the emerging interest in a global solution with federated nodes is best accommodated in this way.

We conclude that the proposed global identification system satisfies all known elements of regulators' requirements for the LEI. It also lays the foundation for further rulemaking and issues yet to be addressed for contract and instrument identification, financial event identification and data aggregation of valued positions and cash flows for systemic risk analysis, the ultimate objective of the rulemaking.

Below is a summary of the key features of our proposed LEI framework which, through the newly formed Regulatory Oversight Committee, is under consideration for implementation by sovereign governments and their financial regulators.

---

[16] See Financial Stability Board, Recommendations for the Global Legal Entity Identifier System (GLEIS) at http://www.financialstabilityboard.org/publications/r_120608.pdf

[17] See footnote 3

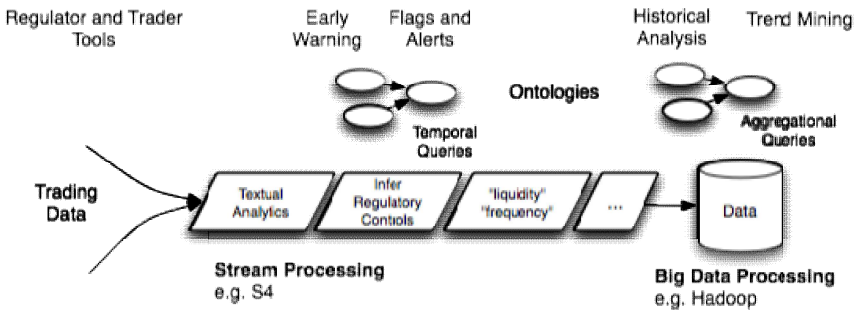
Key Features	Proposed Solution	
	Description	Comments
Scope of Coverage	• The proposed solution supports all aspects of the global Legal Entity Identifier (LEI) initiative as mandated by the G20 via the Financial Stability Board (FSB) • It provides the technological and operational framework to satisfy the initial requirement for the registration, validation and maintenance of information relating to unique legal entity identification (LEI) across the globe for all Financial Market Participants (FMPs) • It has been designed to extend this capability in the form of either an implementation or in releasing open source specifications to others for: o unique product identification (UPI), o unique transaction (swap) identification (USI), and o unique financial (corporate) event identification (FEI)	The proposed solution creates the LEI facility by which global and sovereign regulators that are aligned to the Financial Stability Board (FSB) and the Regulatory Oversight Committee (ROC) can observe and limit accumulations of FMP exposures as a means to more effectively manage systemic risk
COU (Central Operating Unit)	• The proposed solution supports both the Centralized Operating Unit (COU) and the associated Local Operating Units (LOUs) • As each LOU is on-boarded, the COU randomly chooses and then distributes a range of codes to each LOU • These codes are unique globally and are assigned at the consolidated business entity/ control entity (ultimate parent) level • Its random choice method is programmed never to produce a duplicate code	The COU acts as the control mechanism for assignment of code-sets to LOUs that in turn dispense codes as each ultimate parent business entity / control entity requests pre-registration. The resulting code formats are uniform and consistent allowing rapid access to entire sets of LEIs per entity with no mapping tables required.
Code Structure	The proposed solution has a two part LEI code construction, fully compliant with the ISO 17442:2012 LEI standard: 1. First portion: Registration Identifier (RID) administered by sovereign or regional regulators, Local Operating Units (LOUs), each within their own jurisdictions, assigned directly to requesting business entities at the ultimate parent business entity / control entity level 2. Second portion: Self-assigned by each registered business entity to identify each of its operating units or subsidiaries subordinated to the ultimate parent business entity / control entity	The proposed solution facilitates: 1. Control and confidentiality exercised by sovereign states 2. Establishment of business hierarchies with consolidated group level control structures 3. Remote control and synchronization of individual operating units / subsidiaries within each ultimate parent business entity / control entity 4. Maintenance of LEI reference data and changes to ownership status relative to corporate actions of recorded LEIs. In a globally federated network the various codes used by multi-national companies will number in the hundreds and many in the thousands per entity, spread across multiple LOUs. The RID portion of the code will be used for quick access and aggregation of multiple LEIs under different categories of control structures.
Self Registration	The proposed framework requires that each counterparty or issuer of securities or contract market operator or other financial market participant is exclusively responsible for identifying itself through its initiating documentation: articles of incorporation, broker/dealer license, bank charter, or account opening forms with a financial institution	The financial market participant is best positioned to ensure that complete and accurate data is registered

Key Features	Proposed Solution	
	Description	Comments
Certification	The proposed framework requires that the identity of financial market participants is validated by an independent trusted agent identified relative to each sovereign domicile, e.g. auditors, law firms or other designated certifying agents that compares initiating documents to information tagged prior to legal entity registration	Provides assurance that data registered in the GLEIS is maintained in a complete, accurate and timely manner with oversight provided by qualified third parties who understand local laws and practices and can translate them into GLEIS requirements. The proposal is that auditors are the preferred certifying agent as they have a privileged place in understanding business hierarchies and ownership structures and could be relied upon to ensure information in the GLEIS is accurate as part of their standard auditing procedures.
No Intelligence	The proposed LEI codes have no intelligence, i.e. no country or issuing agency code, no ability to parse the number to determine meaning	This ensures the persistence of the LEI (see 'Persistence' below) by requiring that all changes are reflected in the reference data, not the LEI coding
Persistence	The proposed framework ensures that all changes relating to a legal entity are reflected in the associated reference data	If changes are applied exclusively to the reference data, the LEI code remaining unchanged, then the LEI code can persist in perpetuity thereby providing an audit trail for any and all changes. This does not mean that, for example, a merged company cannot be assigned a new LEI code; it only means that in such circumstances the old LEI code is retired, never to be used again. A retired LEI code remains associated with the new LEI code as an audit trail relating to a corporate event.
Confidentiality	The LEI itself need not be confidential but there may be a requirement by sovereign states or governments to ensure parent / child relationships and ownership structures are maintained confidentially. The proposed solution accommodates this requirement through redaction algorithms administered at the source of self-registration.	Sovereign regulators and exchanges (and their auditors) are privileged observers of this information and would be best positioned to protect globally agreed and locally regulated LEI confidentiality rules by administering the registration process and invocation of the algorithm
Federated vs. Centralised	The proposed solution has adopted sophisticated and state-of-the-art technology by overlaying the LEI network as a virtual private network (VPN) 'tunnelled' through the Internet. The Internet itself has been built with inherent resilience there being no single point of failure and thus provides optimal conditions as the network architecture and at the application layer.	In a federated VPN model a directory of LEIs can be replicated so there is no single point of failure as demonstrated in the world wide web's Domain Name Server (DNS) network on the internet. There are many servers available that can, for example, resolve an LEI into an address to locate its LOU. Each server in the DNS network contains or can access the same directory.
The Network Card and the Plug-in Architecture	As required by the FSB the local federated LEI Registry has been designed using sophisticated and state-of-the-art technology around a 'network card' and 'plug-in' architecture at the LOU level that will federate up as the logical virtual database overseen by the Central Operating Unit (COU)	Software at the application layer will aggregate business hierarchies while redaction algorithms mask identification when required by local law or practice. Software anchors will be deployed in local servers (each LOU's LEI registry) to allow access via Automated Program Interfaces (APIs) or Service-Oriented Architectures (SOAs) to multiple vendor products, tools and services in keeping with the requested non-discriminatory and freely available use of LEIs. This technique permits any vendor to offer its services and plug their own hardware, software and other technology into the 'network card' based on the local registration authority's preferences and bidding process.

Appendix 3

Financial Industry Ontologies for Risk and Regulation Data (FIORD) Platform for Risk Analysis

The FIORD platform introduces an innovative approach to analyzing risk triggers to observe the contagion of systemic risk arising in the interconnected financial system.



Gathering, querying and analyzing various types of large data sets is an area that has developed in recent years as the volume and complexity of financial data has grown. This has led in turn to the concept of 'Big Data' that is strongly anchored within collaborative networks concepts. The Financial Services sector is amongst the most data driven of industries. However, the industry has relied on older technologies to handle this ever-increasing data and analytics burden. The regulatory environment for this industry requires an understanding of multiple types of data including: prices, valuations and cash flows; algorithmic trading and risk management models; order and trade execution data; market data for bids and offers, last sales and volume information; order book information; news and economic data; post trade data such as trade allocation information and payment and settlement instructions; corporate event notifications; creation and continuation data for derivatives; and data on financial products, counterparties and other financial market participants.

These datasets result in large volumes of data - billions of market related messages, industry related economic information, and data on individual company and contract markets distributed globally in real time. As an example, just the market data feeds expressing bids and offers distributed on just the below listed equity and options exchanges in the US on a most recent and typical day April 25, 2013 peaked at 5.51 million transactions a second. Historically, the peak rate was 6.8 million per second achieved on December 21, 2012.

The changes in regulation, the increased interconnectedness of markets globally and the concomitant increases in financial data have resulted in a number of problems for financial participants and their regulators:

- The growing number of trading markets to be monitored,
- Non standardized data structures and overloaded middleware techniques;
- Outdated legacy technology solutions – both hardware and software;
- Lagging people and organisation skills in the technology, business and scientific communities necessary to understand 'Big Data', and,
- Finding the right data or combinations of data that will answer a business or scientific question from a very large volume of data in real-time.

Coupled with the above more generic big data challenges is the reluctance of financial services participants to move from their trusted existing IT infrastructure. Thus, an organisation such as a bank may have multiple parallel systems that have different internal data structures. Something of the nature of a paradigm shift in thinking is required. This is what our research and the FIORD platform is aiming towards. More specifically our aim is to allow for these existing platforms to be kept in place, reengineered over time but, in the interim allow for a common definition of the data within the systems to exist enabling a convenient and efficient way to access this data using new tools and methods. We refer to our approach as the FIORD platform

Big data technologies and federated network elements will be required to store and analyze vast amounts of data. This will be done in two parts.

Stream Computing:

This is a high-performance computer system component that analyzes and collates multiple data streams from many sources. In this context the streams of data will be:

- Feeds of data from exchange providers – e.g. NYSE MKT OpenBook which provides a real-time view of the New York Stock Exchange's limit-order book for all NYSE-traded securities. To save substantially on costs but to prove the concept is viable, delayed data will be used in the demonstrations of the platform. Industry users will then be able to use their existing data subscriptions in the final implementation of the platform;
- Internal feeds of data from the individual industry members. This would include risk reporting data such as pricing, valuation and cash flows; order books, executed trades, fail trades and other market data; and, other data such as Legal Entity Identifier (LEI) data as it become available.

As previously discussed the LEI is an initiative to identify all financial entities, including counterparties involved in the financial services market. As became clear during the 2007 onwards financial crisis, no such identifier exists.

The Stream Computing elements of the platform would process the data using an inference engine to find patterns and pre-identified triggers in the data and stream it back out as a single flow. Stream computing uses software algorithms that analyze the data in real time as it streams in to increase speed and accuracy when dealing with data handling and analysis. A challenge for the FIORD platform designers will be to create and test algorithms that can process a large number of streams in real time without any lag. For example if 100 data streams are being analyzed per second but the results are not available for a minute, then the platform will have failed to deliver real time, stream based big data analysis.

Stream Computing Algorithms and Performance

A streaming algorithm is an algorithm that receives its input as a “stream" of data, and that proceeds by making only one pass through the data. Streaming algorithms are designed to be fast and use as little memory as possible.

A model for these algorithms follows:

1. Stream: m elements from universe of size n, e.g. <x1, x2, …., xm> = 3,6,7,4,2,…
2. Goal: Compute a function of stream, e.g., median, number of distinct elements, longest increasing sequence.
3. Problems:
   1. Limited working memory, sub-linear in n and m
   2. Access data sequentially
   3. Process each element quickly

The performance of an algorithm that operates on data streams is measured by three basic factors:

- The number of passes the algorithm must make over the stream;
- The available memory; and,
- The running time of the algorithm.

FIORD designers will explore different existing stream algorithms on the platform to discover which gives the most efficient performance.

The key platform capabilities may include such techniques and software components as:

- Apache Hadoop, an open-source software framework that supports data-intensive distributed applications; this will allow the platform to store any data type in the low-cost, scalable Hadoop engine to lower the cost of processing and analyzing massive volumes of data.
- Apache S4, a general-purpose, distributed, scalable, fault-tolerant, pluggable platform that allows programmers to easily develop applications for processing continuous unbounded streams of data. This will allow the platform to continuously analyze massive volumes of streaming data with sub-millisecond response times to take action in real-time.
- Text Analytics: This would analyze textual content to uncover hidden meaning and insight in unstructured information. The CiCui system from Trinity College Dublin could be used for this. Another alternative is General Architecture for Text Engineering or GATE. This is a Java suite of tools originally developed at the University of Sheffield and now used worldwide for all sorts of natural language processing tasks, including information extraction in many languages.

Using this element of the platform FIORD would be able to uncover patterns of trading, leverage and asset crowding that will give regulators insight into triggers of systemic risk exposures. A suggested early focus for the FIORD project is High frequency Trading (HFT) systemic risk exposures.

Historical Analysis:

In addition to processing data in real time, the streams will be stored in vast storage arrays to allow their review. For example, FIORD could take the triggers identified for systemic risk and see how they stand up to the historical data record as well as use them to proactively give signals of preventive measures. The additional platform element for this would include Data Storage. The preferred solution for this will be huge hardware arrays such as that provided by EMC's symmetric processing clusters, Teradata's multi-array platform, SAP's cloud environment and other such Big Data configurations.

It may be practical in today's technology environment that federated networks of servers across a vast, globally interconnected network as envisioned by the LEI initiative of the G20's Financial Stability Board may provide possibilities to use hundreds of servers as a clustered virtual computing environment.

Big Data analytics can be performed with the software tools commonly used as part of advanced analytics disciplines such as predictive analytics and data mining. But the unstructured data sources used for big data analytics may not fit in traditional data warehouses. Furthermore, traditional data warehouses may not be able to handle the processing demands posed by Big Data. These technologies form the core of an open source software framework that supports the processing of large datasets across clustered systems.

Semantic Platform

The above approach will require a web semantic platform to allow it to link data from diverse sources together, reason over it, federate it, and query it. The key platform capabilities may include:

- Querying: SPARQL is an RDF query language, that is, a query language for databases, able to retrieve and manipulate data stored in Resource Description Framework format.
- Ontologies: OWL or the Web Ontology Language, a language for describing and sharing ontologies on the World Wide Web. This will allow the ontologies developed as part of FIORD to be authored and distributed.
- Rules: RIF is the W3C Rule Interchange Format. This is an XML language for expressing rules which computers can execute.
- Taxonomies: RDF is a set of classes with certain properties using the RDF extensible knowledge representation language, providing basic elements for the description of ontologies, otherwise called RDF vocabularies. These resources can be saved in a "triplestore" to reach them with the query language SPARQL.
- Reasoner: This is software that infers logical consequences from a set of asserted facts or axioms.

Cloud Computing

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). A set of end user tools will be developed to allow data to be gathered from existing computational and communication infrastructure. In turn end users will be able to access cloud-based applications through a web browser or a light-weight desktop or

mobile application. This will include querying of big data analytics using existing reports, including visual representations of data. Alerts of critical events and risk triggers will be sent out to users. The cloud services will be designed to allow for existing data sources to connect and share data with the FIORD platform.

Intelligent Network

The FIORD platform leverages the networked solution of the LEI registries of the Financial Stability Board's Global Legal Entity Identifier System described in Appendix 2 to perform systemic risk aggregation. It requires each LEI register to conform to specifications for a 'network architecture' and 'plug-in card' envisioned by the FSB, not unlike how the architecture of the Internet interoperates. The FIORD platform recognizes that the only place the complete and timely set of LEIs will be updated and stored is in the Global LEI system (GLEIS), a federated global LEI registry network which is to be locally administered (through Local Operating Utilities – LOUs) in home country jurisdictions. This is also where risk data associated with financial transactions under sovereign home/host country risk regimes are to be sourced from, making the LOUs a natural place to aggregate this data locally and, in turn, make risk data available globally through the same virtual data-basing and intelligent network concept envisioned by the FSB for the LEI.

The 'concept' of an intelligent network has its roots in early work on semantic networks where meaning through data tags is imparted to the data that flows through it. A lot of this work was conducted and still is conducted in the military and intelligence communities. The systemic risk and straight-through-processing (STP) application of an intelligent network has its roots in early work conducted by Financial InterGroup and its partners going back nearly a decade.

Before that it had its roots in work done nearly two decades ago by Professor Grody, the founder of Financial InterGroup, while establishing and teaching a Risk Management Systems course at NYU's Stern Graduate Business School. The key elements of an intelligent semantic real-time financial network was presented earlier by a partnership of Financial InterGroup and GS1 (the overseer of the numbering convention in the bar code) to the SEC, the CFTC, and the US Treasury's Office of Financial Research. This was in response to these three agencies' separate solicitations of interest in late 2010 in a global identification system and its first use in swaps regulation and data reporting. Its expected final objective was as a tool to aggregate counterparty and product data for systemic risk analysis.

Most recently this work and the evolving LEI network were proposed to the European Union (EU) as the backbone of an intelligent semantic network. The network is referred to as Financial Industry Ontologies for Risk and Regulation Data (FIORD) proposed under the EU's Seventh Framework Program (FP7) for Research. The proposal was submitted on April 26, 2013 by a consortium of European Universities, financial institutions and technology companies. Its aim is to provide novel algorithms, software infrastructures and methodologies for real time interaction, visualization, analytics and decision support applications over extremely large volumes of data (both structured and unstructured).

Financial InterGroup's CEO, Allan Grody, is Chairman of the Advisory Board for this effort.