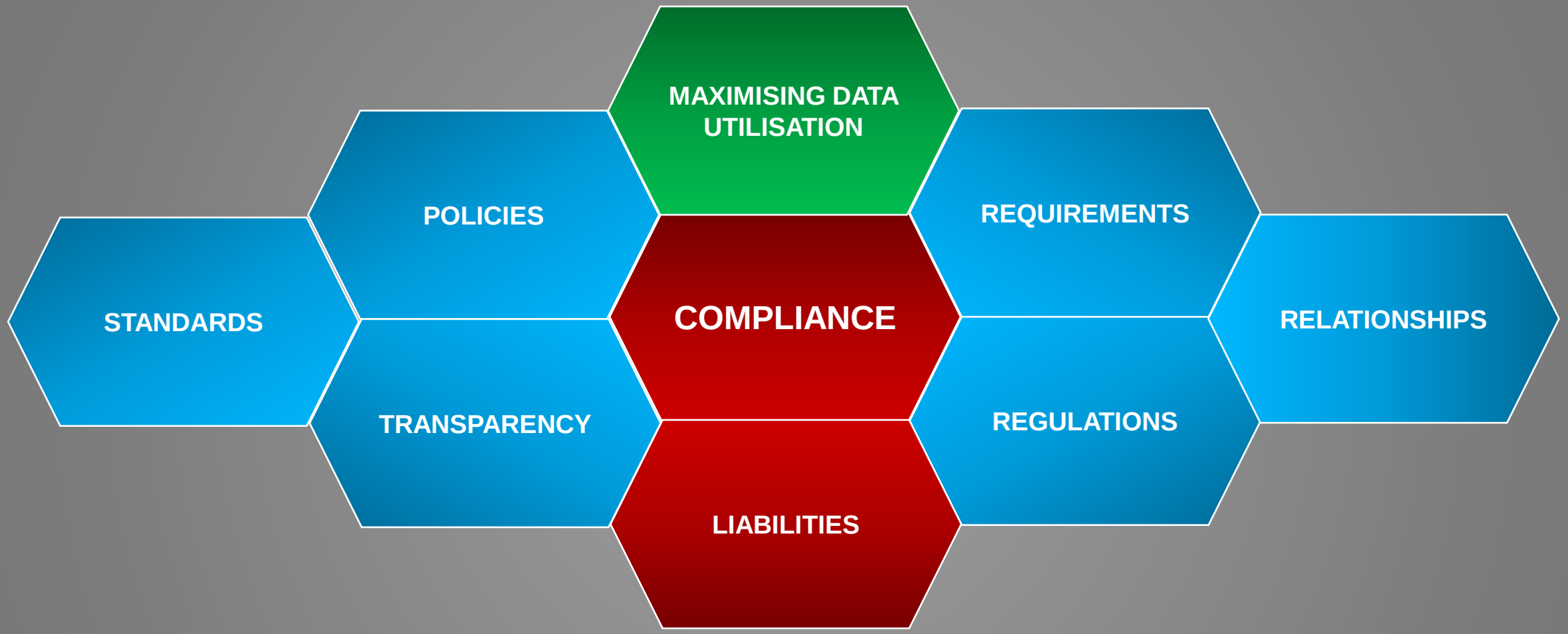


Market Data Audit Defence Services

DataCompliance LLC

Market Data Audit Defence Service

DataCompliance LLC

Introduction

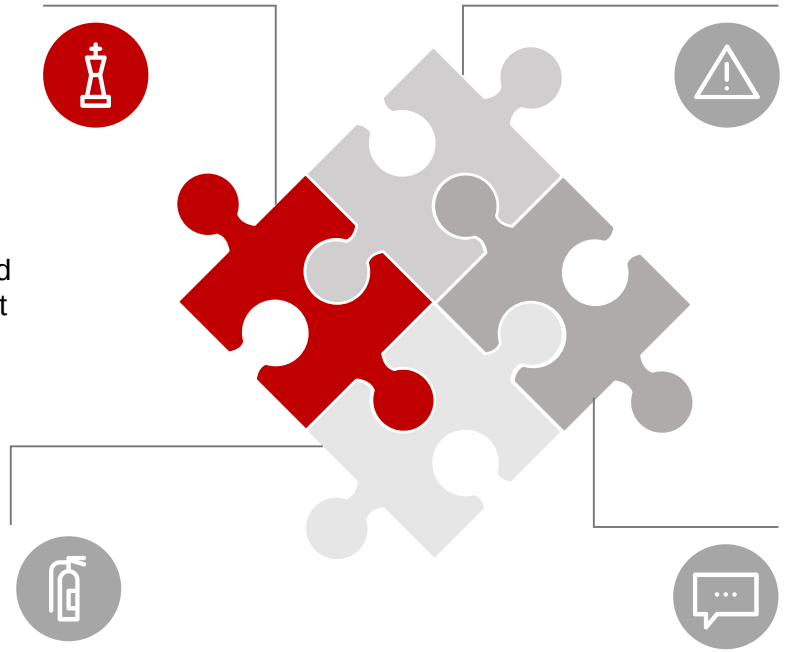
Being licence compliant is expensive, not being licence compliant is <u>much more</u> expensive. Best practice audit defence is based upon preparation, analysis, and the correct application of licence policies based upon the practical knowledge of the client's business and how our clients use and manage its market data services.

In the market data world, over a three year audit period, **the potential for a business to accumulate licensing liabilities is significant.**

Why do Audits happen?

Data is valuable

Mission Critical. Efficient tracking of data pathways creates understanding of creation, ingestion, consumption and distribution by feeds, systems, applications, and terminals in all its different frequencies and formats, e.g. real-time, derived, delayed.



Reporting methods

Accuracy. Even today market data reporting can be based upon manual processes, declarations and 'honesty statements'. Auditing is therefore a natural part of the process, i.e. identifying any potential errors.

Resolutions

Identify, understand why, then eliminate any, and every, errors of non-compliant usage and distribution.

Effective communication

Best practice audit defence is built upon the better application of policy understanding and improved on-going compliance.

Dollar Facts

The following are examples of average liabilities banks incurred between 2014 and 2017 after exchange audits:

Tier 1 Investment Bank: **$16 Million**
Tier 1 Global Bank: **$10 Million**
Tier 2 Global Bank: **$7 Million**
Tier 2 Domestic Bank: **$4 Million**

Market Data Audit Defence Service

Our approach

DataCompliance LLC

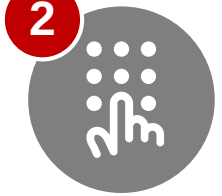
As data is utilised further away from sources, the control of, monitoring of, and sight of usage, diminishes so creating potential licensing liabilities. DataCompliance uses this knowledge to help guide our approach to market data audit defences.

The following are **four key areas** for our audit defence:

1

In-House Usage
Focusing on electronic trading services, all other display & non-display applications data derivation, original works creation and terminal based applications. *Verification of usage compared to an exchange's findings.*

2

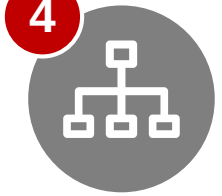


Reporting Systems
Data usage in risk management systems, portfolio management systems, client reporting, regulatory reporting and in-house data storage. *Assess accuracy of an exchange's findings.*

3

Management & Data Tools
Consists of data reporting tools, permissioning and entitlements alongside data inventory management. *Validate an exchange's findings against actual usage*.

4



Data Re-Distribution
Encompasses redistribution to external and internal sources. This increasingly involves third party data processing typically by ISVs. *Ensure comprehensive analysis of overall usage.*

Note: This should include all data sourced from exchanges, brokers, other sources, and original works creators (Indices, ETFs & Structured Products) distributed to and by all vendors, sub-vendors, ISVs and end user firms, real time and non-real time data, alongside data used for pricing and reference services, including historical, derived, retail, professional, intra/extranet.

Market Data Audit Defence Service

Why DataCompliance?

DataCompliance LLC

Market data audit defences require **two way conversations**. DataCompliance effectively communicates between data sources, exchanges and our clients, providing a willingness to listen, and a sensible approach thus bringing a new strength to the relationship. This methodology has been based on DataCompliance's extensive licensing management and auditing experience.

Market Data Expertise

DataCompliance has extensive experience in the field of market data. This includes real world business usage, data governance, contract management, sourcing, cost optimisation and exchange data management. We draw upon our experience to provide significant value.

Technical Knowledge

An in-depth understanding of the systems and management processes required, including regulatory workflows, enterprise strategy and reporting data governance.

Diplomacy

The ability bring two parties together when negotiating potential liabilities introduces new dynamics. When required an audit defence is a negotiation between two parties; effective negotiation is a core audit defence strategy facet.

Contractual Knowledge

Expert understanding of the policies and agreements in place is a prerequisite. Experience enables us to provide interpretational analysis of policies and contracts on a policy-by-policy basis, and their practical application with peer groups.

Communication

Effective communication between parties is a requirement. We will agree upon a communications strategy.

Clarity

Market data policies can be misunderstood, also wilfully misunderstood, even by those applying them. So transparency, and flexibility in interpretation and the explanation of findings is a necessity. The ability to be candid, concise and accurate, is supported by effective communication skills, contractual and technical knowledge.

Market Data Audit Defence Service

DataCompliance LLC

Our principles

There are **key compliance and audit principles** which work toward the successful conclusion of each management review, analysis and audit, contributing to risk reduction and dollar mitigation. At DataCompliance there are no conflicts of interest.

Neutrality

DataCompliance works with industry participants. The consultants will protect confidential information and not prejudice the client in any audit defence.

Conflict of Interest

Any potential conflict of interest will be made known to all parties before any project work can commence.

Liability Calculations

Based on information made available, each liability calculation must be as accurate and exact as possible for internal assessment or for any audit periods under examination. DataCompliance verifies and validates all potential liabilities found externally and internally.

Exceptions

Analytical extrapolations may be required and analysed if insufficient information is made available. Each extrapolation calculation must be reasonable, explained and clear.

Requests for Information

All information requested must be made available in a timely manner with set deadlines. Reasonable request for delays are acceptable subject to an agreement from yourselves.

Audit Negotiations

Discovering correct potential liabilities by internal assessment or for an entire period reduces the requirement for negotiation by our clients, therefore this must be the objective. DataCompliance validates the correct and proper application of policies by each of the clients' data providers.

Audit Client Interaction

At all stages, all the parties involved must be kept informed of progress in a timely manner, and of any issues addressed at the point of occurrence or knowledge.

Audit Timeframes

Audits, internal and external, are a drain on resources for all parties, therefore it is imperative to ensure a timely and accurate completion with recourse to debate and negotiation.

On-going Relationships

Each party must retain on-going relationships; each audit must be conducted on the basis of protecting and enhancing these relationships. Fairness of application is fundamental.

Market Data Audit Defence Service

Proven Methodologies

DataCompliance LLC

The **five phases** outlined in the timeline are expanded upon below

1 Audit Planning

- Prepare for the internal and/or external audit by reviewing the applicable policies chronologically and the nature of the requirement.
- Set deliverables and assess project requirements.
- Set criteria for success and end state.

2 Discovery

- Analyse the exchange's findings and verify, or otherwise, the material application of the exchange's own policies related to those findings.
- Cross check findings to internal documentation.
- Validate and verify data source and vendor records.
- Understand our clients' business relative to their markets, how they trade, their market data environment, which re-distribution channels are used and subscription levels.
- Identify key internal relationships, and stakeholders.

3 Audit Defence Process

- DataCompliance Market Data Compliance Dashboard visualises audit defence analysis from start to finish.
- Prepare final internal analysis and audit checklist.
- Identify risk factors alongside identifying any exceptions as well as identify and report data usage outside of data policies.
- Conduct technical and analytical audits where usage can be clearly documented through the use of entitled systems.
- Conduct a non-technical audit where usage cannot be physically measured.

4 Feedback and Follow up

- Interpret and extrapolate all findings.
- Produce interim report which identifies all outstanding issues.
- Work with the client to mitigate and eliminate all outstanding issues.
- Identify and advise on implementation of best practice solutions.
- Assess management and relationship. Are there areas for improvement?

5 Conclusion

- Produce final report identifying successful resolutions of issues raised in the interim report.
- Document if the analysis and audit did not meet the success criteria. If it did not, address why it did not and provide recommendations moving forward.
- Final report is aimed at delivering best practice future compliance management.

A 'live' dashboard for a 'live' environment

Market Data Audit Defence Service

Our deliverables

DataCompliance LLC

A clearly defined report structure comprising the following. For each analysis and audit there are **two reports**:

1

Summary Report
- Summary of the findings
- Assessment of all potential liabilities compared to original findings
- Description and calculation of the correct liabilities

2

Full Report
The full report includes the summary, plus additional details, analysis with all relevant background information alongside the following:
- Introduction, conclusions, details, verification and validation of all findings compared to the original exchange calculations
- Strategy and tactics to ensure compliance to avoid future liabilities
- Negotiate liability findings if required
- Strategic objective: reduce audit liabilities to the correct minimum

Market Data Audit Defence Service

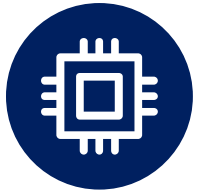
The analytical process

DataCompliance LLC

DataCompliance undertakes due diligence by requesting key documentation and information in advance of our analysis. This streamlines the process and creates the evidence.

Documents and Processes

- Entitlements/Permissioning. Review of systems diagrams, and usage reports for the control of, monitoring of, and reporting of usage.
- Identify how data services are documented and codified internally



Explanations

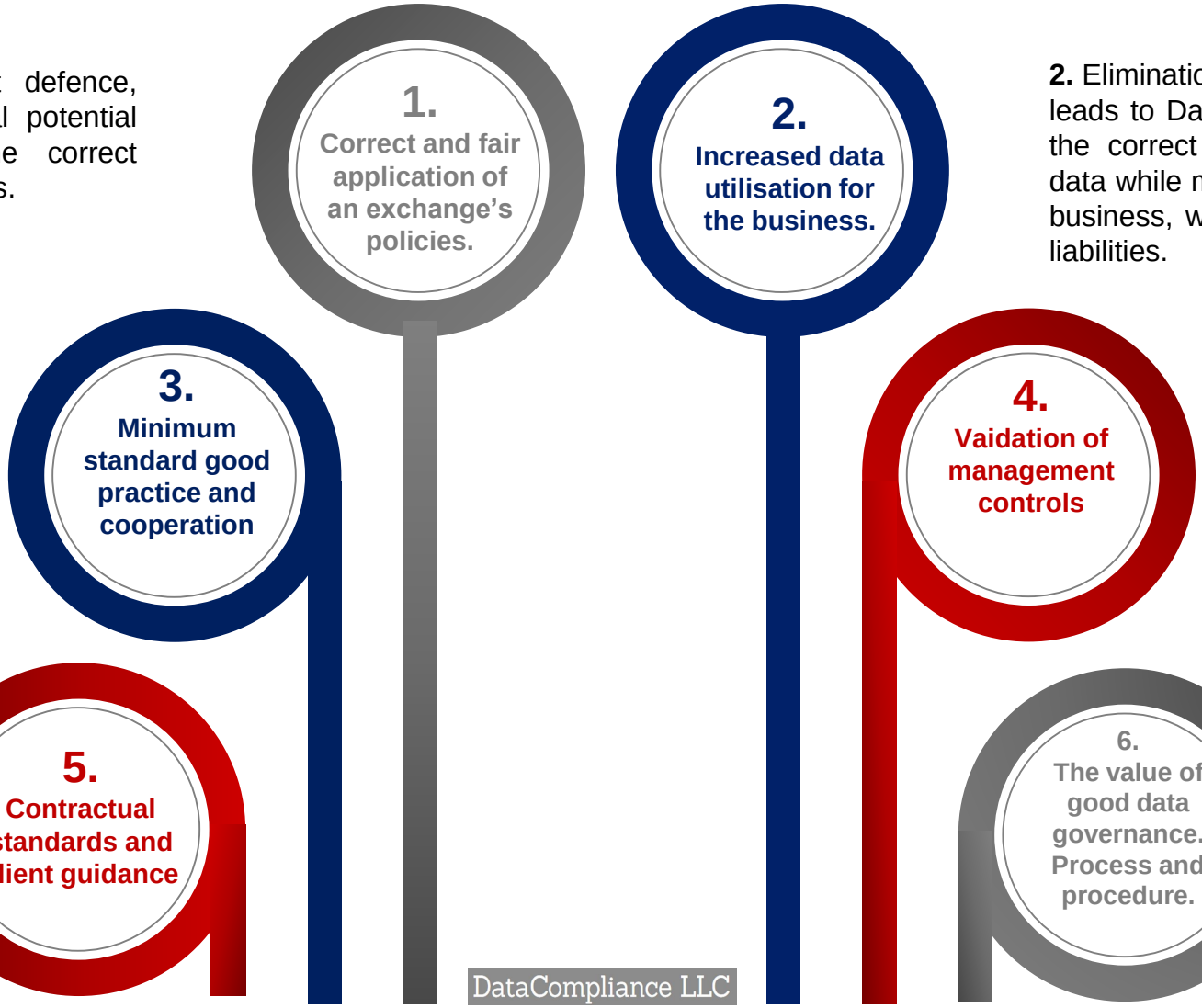
- Review external assessments of potential liabilities, including validation and verification of the correct application of policies and the calculated findings as required
- Review existing management processes and procedures
- Analyse invoicing, mapped to reporting
- Technical explanations as to how the permissioning and distribution systems function and connect to service facilitators/end-users (documented) with a practical demonstration to validate access
- Access to the enablement/permissioning database to check against what has been reported previously.
- Access to documentation detailing how data is coded for sales/reporting purposes
- Is, or has in the past, any usage which for whatever reason has not been reported? If so, why?
- When are the cut-off times for reporting?
- Information on how many internal IDs are being used at service facilitators' or within the business for different purposes

Market Data Audit Defence Service

The benefits

DataCompliance LLC

1. As part of the analysis/audit defence, DataCompliance identifies the real potential dollar liabilities based upon the correct application of an exchange's policies.



2. Elimination of any discrepancies in usage, leads to Data Sources/Exchanges receiving the correct and fair payment for licensed data while maximising data utilisation for the business, while minimising costs and dollar liabilities.

3. A minimum standard of good practice and co-operation between the parties to an audit, i.e. verification of contractual obligations between the Exchanges and the disseminating Vendors.

4. Validation of the data management processes and technical controls in place for Controlling, Monitoring, and Reporting data usage to ensure ongoing compliance.

5. Advising our clients on contractual clarification, definitions, terms and conditions**,** considering that exchanges and data sources lack common standards.

6. Maximising value in data usage, minimising and eliminating audit liabilities either through audit defence or internal identification of potential liabilities is built upon good data governance foundations.

Market Data Audit Defence Services

Success Stories

DataCompliance LLC

Case Studies

DataCompliance LLC

These are 3 case studies of 3 previous audit defence engagements. DataCompliance will provide more case studies upon request.

Client: Tier 1: UK Commercial Bank

Project Scope: Data Governance & Services Application Usage Review. Analysis of the client's enterprise usage of Market Data within applications (i.e. Risk, Trading Platforms, Venues, Client and Regulatory Reporting), assess costs and identify potential non-compliant usage, and review data governance of market data services including pre- and re-qualification of data.

Key Achievements:

- Identified £5.5 million of liabilities (subsequently proven to be 92% accurate).
- Identified control, monitoring and reporting deficiencies.
- Proposed changes to management and administration structures.

Clients: Tier 1 US Brokerage

Project Scope: Multi-Million Dollar Audit Defence against 2 Global Exchanges. Analysis of exchange findings, presentation of detailed report and assessment of the validity and accuracy of each finding made by the exchanges. Reviewed internal policies for permissioning and entitlements systems for control, monitoring, and reporting of data usage.

Key Achievements:

- Reduced initial audit findings by 65%.
- Analysis identified where the exchanges provided incorrect evidence.
- Identified incorrect application of each exchange's policies.
- Negotiated agreed settlement with each of the two exchanges.

Client: Tier 1 US Market Data Vendor

Project Scope: Multi-Million Dollar Audit Defence against 1 Global Exchanges. Due Diligence comprising information discovery, collation, and analysis to determine current situation. Presentation of report and advising the client on negotiation strategies. Presentation and explanation of findings to the exchange, and negotiating the mitigation of liabilities.

Key Achievements:

- Reduced initial audit findings by 100%.
- Identified incorrect application of the exchange policies.
- Ensured exchange agreed there were zero liabilities.
- Negotiated an agreed no audit agreement for a specific period.