LLOYD'S

Lloyd's Minimum Standards MS11 – Cyber Security and Data Management

January 2019

Contents

MS11 – Cyber Security and Data Management 3

Minimum Standards and Requirements 3

Guidance 3

Definitions 3

Section 1: Cyber Security and IT Infrastructure 5

Section 2: Data Governance Framework 7

Section 3: Systems and Processes 8

Section 4: Reporting and Quality Control 9

APPENDIX – LINKS 11

MS11 – Cyber Security and Data Management

Minimum Standards and Requirements

The Minimum Standards are statements of the business conduct required by Lloyd's, established under relevant Lloyd's Byelaws. The Requirements represent the minimum level of performance required of any organisation within the Lloyd's market. All managing agents are expected to comply with the Minimum Standards.

Within this document the standards and supporting requirements are set out in the blue box at the beginning of each section. The remainder of each section consists of guidance which explains the standards and requirements in more detail and gives examples of approaches that managing agents may adopt to meet them.

Guidance

This guidance provides a more detailed explanation of the general level of performance expected. It is a starting point against which each managing agent can compare its current practices to assist in understanding relative levels of performance. This guidance is intended to provide reassurance to managing agents as to approaches which would certainly meet the Minimum Standards and comply with the Requirements. However, it is appreciated that there are other options which could deliver performance at or above the minimum level and it is fully acceptable for managing agents to adopt alternative procedures as long as they can demonstrate how these meet the Minimum Standards.

Definitions

Catastrophe Modelling: (also known as cat modelling) is the process of using computer-assisted calculations to estimate the losses that could be sustained due to a catastrophic event such as a hurricane or earthquake.

Delegated Authority: all forms of business where underwriting and claims authority has been delegated to another entity (e.g. binding authorities, consortia, lineslips etc.).

KPIs: Key Performance Indicators

LCM: Lloyd's Catastrophe Model

Lloyd's Returns: this will include, but not be limited to: Broker Remuneration Return; LCM

Submissions; PMDR; QMB; RDL; RDS; Related Parties Return; SBF; Self-Assessment of Compliance versus Lloyd's Underwriting and Claims Standards; Syndicate Business Plan; Syndicate Reinsurance Programme Return; Xchanging Claims

MI – Management Information

PMDR: performance management data return

QMA: Quarterly Monitoring Return – Part A

QMB: Quarterly Monitoring Return – Part B

RARC: Risk Adjusted Rate Change

RDS: Realistic Disaster Scenario

Related Party: A related party shall mean:

1. Another syndicate managed by the same managing agent or a service company coverholder that is part of the managing agent's group.
2. Any company which has two or more directors in common with the managing agent

3. Any company within the same group as a corporate member of the syndicate which has a member's syndicate premium limit of more than 10% of the syndicate allocated capacity
4. Any company within the same group as the managing agent

SBF: Syndicate Business Forecast

Syndicate Business Plan: means a business plan prepared by a managing agent in accordance with paragraph 14A of the Underwriting Byelaw.

PRA – Prudential Regulation Authority

The Board - Where reference is made to the Board in the standards, managing agents should read this as Board or appropriately authorised committee. In line with this, each agent should consider the matters reserved for the Board under the Governance Standard in order to evidence appropriate full Board discussion and challenge on the material items.

Underwriting Data: this will include, but not be limited to all data which the managing agent, Lloyd's or other appropriate regulators require to monitor the business with regard to underwriting activities.

Section 1: Cyber Security and IT Infrastructure

CDM 1.1 Cyber Security and IT Infrastructure

Managing agents shall have appropriate IT systems and resilience for the management of the agency.

Managing agents shall:

- have appropriate IT infrastructure to manage the business; and
- have appropriate IT techniques in place and be annually Cyber Essentials accredited to reduce the operational risk of cyber-attack.

The LMA cross Market cyber forum has considered that Cyber Essentials or Cyber Essentials Plus is an appropriate level of accreditation to reduce the risk of a Cyber Attack.

Lloyd's has set the minimum requirement for an agent to be Cyber Essentials compliant. It is not expected that this will be the only protection that an agent has in place. In some cases the agent will be Cyber Essentials Plus accredited, or meet the NY Department of Financial Services (DFS) Cybersecurity Requirements for Financial Services Companies; others may have bespoke solutions.

Cyber Essentials concentrates on five key control themes. These are:

1. **Boundary firewalls and internet gateways** – these are devices designed to prevent unauthorised access to or from private networks, but good set-up of these devices either in hardware or software form is important for them to be fully effective.
2. **Secure configuration** – ensuring that systems are configured in the most secure way for the needs of the organisation.
3. **Access control** – ensuring that only those who should have access to systems do have access and at the appropriate level.
4. **Malware protection** – ensuring that virus and malware protection is installed and is up to date.
5. **Patch management** – ensuring that the latest supported versions of applications are being used and all the necessary patches supplied by the vendor have been applied.

There are two levels of certification – Cyber Essentials and Cyber Essentials Plus. The Cyber Essentials certification is awarded on the basis of a verified self-assessment. The process sees an organisation undertake their own assessment of their implementation of the Cyber Essentials control themes via a questionnaire, which is approved by a senior executive such as the CEO. This questionnaire is then verified by an independent certification body to assess whether an appropriate standard has been achieved, and certification can be awarded.

Certification at this stage is intended to provide a basic level of confidence that the controls have been implemented correctly, and relies on the organisation having the skills to respond appropriately to the questionnaire.

Cyber Essentials Plus, however, offers a higher level of assurance through the external testing of the organisation's cyber security approach. Tests of the systems are carried out by an external certifying body, using a range of tools and techniques. The assessment can either directly test that individual controls have been implemented correctly or recreate various attack scenarios. The testing covers all internet gateways, all servers providing services directly to unauthenticated internet-based users and user devices representative of ninety per cent of all user devices.

The Government is keen to stress that organisations that are good at cyber security and have a reputation for cyber dependability can use this as a selling point – demonstrating to their customers through the Cyber Essentials badge that they take cyber security seriously.

For more information, visit: www.cyberessentials.org.uk

CDM 1.2 Information Systems and Security

Managing agents shall establish information systems which produce complete, reliable, clear, consistent, timely and relevant information and shall safeguard the security of information.

Information shall cover:

- the business activities;
- the commitments assumed; and
- the risks to which the business is exposed.

Managing agents shall:

- establish and implement an approach to safeguarding the security, integrity and confidentiality of information which takes into account the nature of the information in question; and
- ensure that they meet the requirements of the Data Protection Act 2018, General Data Protection Regulation (GDPR) and any local data protection regulation based on territories in which they operate or have data subjects.

The overall information system should be documented and set out which information is to be shared, by whom, and when and allow for information to flow up and down hierarchy levels as well as horizontally between different business units where appropriate. Managing agents should be able to demonstrate that there is clear linkage between individual information systems (i.e. it should be clear how one system feeds another).

Managing agents should decide who needs to have access to these information systems for the purpose of providing input from and to their areas of responsibility and who the relevant personnel are that need to have passive access to the system so as to retrieve data for the proper discharge of their duties.

Information needs to cover all business activities and commitments assumed across the organisation, e.g. acceptance of underwriting risks, other financial commitments etc.

Data Protection

Managing agents should note that the use of all personal data and information is regulated by the Data Protection Act 2018, General Data Protection Regulation (GDPR) and any local data protection regulation based on the territories in which they operate or have data subjects.

Managing agents are expected to implement appropriate controls to meet the requirements of the General Data Protection Regulation and the Data Protection Act 2018 which superseded the Data Protection Act 1998 and which introduced some derivations to the GDPR regulations.

[Link to the Data Protection Act 2018 and the GDPR can be found in the appendix at the end of the document]

Section 2: Data Governance Framework

CDM 2.1 Data Governance Framework

Managing agents shall ensure that they have data governance structures and procedures in place.

Managing agents shall:

- appoint a nominated director(s) with accountability for oversight of the governance framework for data;
- have appropriate policies and procedures in place to allow timely recording and production of data, the suitability of which are reviewed annually to ensure data returns are appropriate, accurate, complete and submitted on time.
- ensure that the data governance framework allows for regular reporting of data to the Board, relevant committees and Lloyd's; and
- ensure that roles and responsibilities for the management of data are clearly defined, approved by the Board and reviewed annually.

Policies on data governance should be agreed by the Board and should have regard to the data required by the internal function, any external service providers, the PRA and Lloyd's.

The nominated director(s) with accountability for data governance should have a sufficient level of authority and access to resources and information to enable him/her to carry out his/her responsibility.

The data governance framework should capture the structures and procedures, including triggers for escalation, to support the quality of data. Managing agents should have a framework in place which shows clear oversight of the quality of internally produced data, responsibilities and accountabilities. In addition it should ensure appropriate, accurate, complete and timely reporting to support required governance and management decision making processes, together with prompt detection of issues.

Lloyd's expects managing agents to ensure that written data policies, procedures and standards are kept under regular review, at least on an annual basis or where there is a material change impacting the policy such as a change to a stakeholder. These documents should include the responsibilities and accountabilities of the various stakeholders across the managing agent and the quantity and quality of data metrics reported to management.

Data management is often a separate responsibility to reserving and it is required practice that there is a clearly identified owner of the data used. The reserving team should have a strong input into the data that is collected and how it is stored, and should review the data carefully before relying on it. The reserving team should also be aware of, and the reasons for, any adjustments to the data which may have a material impact to the reserve estimates. The reserving team should always be aware of the data provided to Lloyd's and available to respond to queries on this.

The governance in place is expected to include the need for compliance with Lloyd's requirements, including the guidance associated with returns, and deadlines for data returns.

Section 3: Systems and Processes

CDM 3.1 Systems and Processes

Managing agents shall have systems and processes in place to record relevant data and use the output for reporting to management, Lloyd's and other regulatory authorities.

Managing agents shall have systems and processes in place:

- to record data which is sufficient in granularity and coverage to enable the Actuarial Function to appropriately monitor experience and perform forecasting;
- to record data which is sufficient in granularity and coverage to monitor performance against Syndicate Business Plans and forecasts; and
- have appropriate systems and tools in place to enable production of data returns to Lloyd's at sufficient granularity to meet other appropriate external regulatory requirements and guidelines.

Managing agents should ensure that they have systems, modelling tools and analysis methodologies in place to meet the requirements of the business. It is important that systems and processes relating to data can produce timely and accurate management information to executive management, the Board and ultimately to Lloyd's through submissions of returns to Lloyd's.

Relevant data from models and forecasts, i.e. to calculate risk adjusted rate change (RARC), benchmark price etc. must be part of the data infrastructure to allow for data integrity and accuracy to be achieved on Lloyd's underwriting data returns.

Lloyd's expects managing agents to give due consideration to IT systems with regard to data so that the quality and integrity of the data and its processing is not compromised.

Personnel will need relevant skills and experience to ensure that there is:

- familiarity with systems, processes and tools;
- recognition of market groups within the Lloyd's market and external service providers who could assist with data solutions; and
- consideration of any tools / techniques suggested by Lloyd's.

Section 4: Reporting and Quality Control

CDM 4.1 Timeliness, Accuracy & Completeness of Management Information, Lloyd's Returns and Regulatory Reporting

Managing agents shall complete all returns required to Lloyd's and the PRA and ensure that data reported internally and in returns to Lloyd's is accurate, complete and produced in a timely manner.

Managing agents shall:

- ensure that the Board and relevant committees receive regular data reports, including those produced by Lloyd's, to enable management to monitor performance;
- accurately complete returns via Lloyd's Data Collection platforms in accordance with the instructions posted where applicable;and
- ensure the data can be reconciled to the syndicate accounts, Management Information and is consistent with that reported to Lloyd's and other external regulators.

During 2018 Lloyd's improved the technology and processes for the collection of oversight and regulatory data from the market as part of the Market Data Collections (MDC) Programme. MDC has scheduled existing market returns to be migrated onto the platform at the most appropriate times and ensure that this is undertaken to minimise impact to the market stakeholders. Appropriate levels of notice and training will be given in advance further information on specific impacted returns and timelines was published in 2018 directly by the MDC Programme team. Lloyd's Data Collection platforms will continue to evolve and information will be available on the Lloyd's website.

[Link to Market Data Collections (MDC) can be found in the Appendix at the end of this document]

Executive management and the Board should be aware of the returns that are being issued externally to Lloyd's and to regulators.

Syndicates should establish and maintain the necessary arrangements to ensure that consistent and timely electronic delivery of the submissions is possible without material interruption due to human or technical failure.

There is an expectation that reconciliation of returns to internal Management Information and other Lloyd's returns should be available. Lloyd's expects managing agents to be able to demonstrate how the information reconciles and provide an audit trail of any allocation required for Lloyd's returns. Lloyd's will not routinely test returns to other regulators as part of a review of Data Management Standards, but there is an expectation that these should be capable of reconciliation to internal Management Information and Lloyd's returns. Should an issue arise with an external regulator and testing becomes necessary, Lloyd's expect managing agents to be able to demonstrate how the information reconciles.

Reconciliations required as part of submissions to Lloyd's are outlined in the instructions for each return.

The KPIs within reports should be provided at the appropriate levels of granularity to enable the Board and relevant committees to make informed strategic decisions.

Syndicates with delegated authority business of more than 10% must display KPIs to this level of granularity (i.e. binder v non-binder business)

There should be sufficient information to provide clarity on the current position and the likelihood of meeting annual targets (including historical data for comparison purposes can assist with this). Whenever there are changes to Syndicate Business Plans, these are to be reflected in the reporting.

CDM 4.2 Quality Control

Managing agents shall have processes in place to review the systems and controls framework ensuring data is accurate and complete.

Managing agents shall ensure that:

- there is regular exception reporting to identify potential variances or control failures in recording and producing data and these are investigated and escalated;
- the quality of data is continuously assessed to ensure accuracy and completeness; and
- the systems and controls framework for data is subject to regular internal audit review.

Throughout the production process of data, from recording to reporting, Lloyd's expects controls to be in place to ensure accuracy and completeness of data, which can include data error reports / validation reports / exception reports etc. For example, exception reports may address larger premiums or line size, entries with unusual currencies for the syndicate, high acquisition costs, blank data fields where information would be expected to have been entered etc.

There should be a process of checking the quality of data on a timely, frequent and ongoing basis with due regard to the materiality and the potential risk associated with inaccuracies. Where data entry is outsourced, accountability and responsibility remains with the managing agent who should also have a process of quality checking.

Managing agents are expected to have an Internal Audit programme in place. Internal Audit are required to undertake regular reviews of the systems and controls for data for the production of Management Information and returns to Lloyd's and other appropriate external regulatory and accounting returns. For those managing agents who have test processes in place e.g. Sarbanes-Oxley (SOX), they are not considered to be sufficient on its own.

This Internal Audit programme should include:

- Data validation & consistency;
- Data completeness;
- Effectiveness of analysis procedures;
- Process of converting data to Management Information; and
- Reporting accuracy / completeness / timeliness.

Potential evidence

- Data Flows;
- Data Policy;
- Data Procedures;
- Data Exception/Validation Reports;
- Information provided to the managing agency Board and Committees;
- Internal Audit Plan;
- Internal/External Audit Reports on data quality;
- IT Infrastructure;
- Lloyd's Returns;
- Reports from Lloyd's to the managing agent; and
- Structure Chart.

APPENDIX – LINKS

- Data Protection Act 2018 –

  https://www.legislation.gov.uk/ukpga/2018/12

- GDPR –

  https://www.eugdpr.org/

- Lloyd's Data Collection platform - Market Data Collections (MDC) –

  https://www.lloyds.com/mdc