LLOYD'S

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

January 2021

Contents

MS11 – Cyber Resilience 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 if they can demonstrate how these meet the Minimum Standards.

Definitions

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.

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.

Cyber Incident: refers to an event that threatens the confidentiality, availability or integrity of networks, information systems or data of managing agents. It includes a cyber-attack (for example: DDoS, Ransomware, website defacement), any Personal Data Breach or a similar breach of non-personal (commercial) data which includes Underwriting data.

Data Protection Supervisory Authority: has the meaning given in Article 4(21) GDPR

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

GDPR: The General Data Protection Regulation EU 2016/679 in the EU and in the UK, the UK-GDPR as modified by the Data Protection Act 2018

KPIs: Key Performance Indicators

KRIs: Key Risk 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

Material Cyber Incident: refers to a Cyber Incident which may be material if it:

- results in significant loss of data, or the availability or control of your IT systems
- affects a large number of customers

- results in unauthorised access to, or malicious software present on, your information and communication systems.

MI – Management Information

NCSC – UK National Cyber Security Centre, a part of GCHQ

Oversight Manager – Relationship manager and primary contact point for Managing agents, employed by the Corporation

Personal Data Breach: has the meaning given in Article 4(12) GDPR

PRA – Prudential Regulation Authority

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.

Underwriting Data: this will include, but is not 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 Resilience

CDM 1.1 Information Systems and Reporting

Managing agents shall establish information systems which produce complete, reliable, clear, consistent, timely and relevant information and shall safeguard the security of information in a manner that is consistent with CDM 1.2 to CDM 1.8.

Managing agents shall:

- ensure that information covers the business activities, the commitments assumed and the risks to which the business is exposed;
- establish and implement an approach to safeguarding the availability, integrity and confidentiality of information which considers the nature of the information in question;
- notwithstanding any requirement to report a Cyber Incident to comply with any law or regulation, managing agents shall report Material Cyber Incidents to Lloyd's via their designated Oversight Manager as soon as possible after they become aware of the same and within 72 hours at the latest; and
- following reporting, managing agents shall engage in constructive discussions with their designated Oversight Manager and take such steps as are reasonable both to mitigate the effects of the Cyber Incident and to reduce the chances of its reoccurrence.

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 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.

A concern of Lloyd's is to ensure that its Oversight Managers are aware of all cyber security or data breaches (called in this Standard a “Cyber Incident”) that may affect the Lloyd's market. Here, the references to data breaches refers to any kind of data, both personal or commercial. This is of concern to Lloyd's itself, and because others could be affected by the same or a similar Cyber Incident. As such, there is a requirement for managing agents to:

- report Material Cyber Incidents to their designated Oversight Manager as soon as they become aware of the same; and
- engage in constructive discussions with their Oversight Manager and take such steps as are reasonable both to mitigate the effects of the Cyber Incident and to reduce the chances of its reoccurrence.

CDM 1.2 Cyber Governance

Managing agents shall establish an approach to overseeing the effectiveness of cyber risk and resilience management, to ensure Board level accountability, provision of adequate resources and alignment with the organisation's strategic business objectives.

Managing agents shall:

- establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national and industry standards and guidelines;
- ensure that the Board is accountable for the cybersecurity strategy, endorses the managing agent's cybersecurity framework and sets the tolerance for cyber risk;
- conduct annual reviews of the organisation's cyber resilience capability to highlight any material gaps and/or areas for improvement.

Cyber governance refers to the arrangements an organisation has put in place to establish, implement, and review its approach to managing cyber risks. Strong cyber governance will help a managing agent to maintain a systematic and proactive approach to managing the prevailing and emerging cyber risks that it faces.

It also helps a managing agent to appropriately consider and manage cyber risks at all levels within the organisation, as well as consistently bring to bear appropriate resources and expertise to deal with these risks.

A cybersecurity strategy is an essential part of how an organisation sets it's cyber security agenda and ensures cyber risks and identified, evaluated and mitigated in a consistent manner across the organisation.

Steps which management can take to proactively tackle cyber risk and to enhance their cybersecurity framework:

- Deep dives on specific cybersecurity related topics (e.g. undertaken by risk/ second-line functions in conjunction with operational/ first-line departments to improve general awareness & understanding of cyber across the organisation);
- Detailed annual reviews of the organisations' cybersecurity framework against industry standards to highlight any material gaps/areas for improvement and to use the output to formulate the organisations' IT strategic plan;
- Ensuring that the three lines of defence are joined up when carrying out their assurance activities, with evidence of:
    - regular dialogue and interaction;
    - a good level of awareness and understanding of the work being undertaken across the other lines of defence;
    - an understanding of the cyber skills/resourcing within the other lines of defence.
- Comprehensive program of oversight by the third line of defence, including:
    - IT audits to oversee areas with heightened cyber risk;
    - specific proportion of IT audit resource dedicated to undertaking cyber security related reviews or, alternatively, a dedicated team of external support/experts;
    - representation at those forums responsible for oversight of cyber.

Management could also look to enhance the quality of MI through collating a wider suite of key performance indicators (KPIs) and using these to develop key risk indicators (KRIs), being more forward looking and identifying emerging trends, as well as more comprehensive reporting around the monitoring activities undertaken across the organisation with respect to cybersecurity.

CDM 1.3 Cyber Identification

Managing agents shall ensure that they have identification capabilities in place.

Managing agents shall:

- identify key services, processes and underlying systems (networks, applications and data) including third party dependencies, prioritise in order of importance and assess respective cyber risks.

It is recommended that instead of taking a blanket approach to implementing controls across all areas of the business, managing agents could consider taking a risk-based approach, by identifying those services, processes and underlying systems (networks, applications and data) that are critical to its organisation. This will often require a co-ordinated effort between technology and business functions on an ongoing basis.

Following that, managing agents could assess the current internal and external threats, determine the likelihood and impact of a cyber compromise or data breach on those critical services, then develop a set of holistic controls in a proportionate and cost-effective way.

Some organisations have taken steps to appoint full time resource to collate, interpret and disseminate cyber security related threat intelligence (e.g. Intelligence Analyst/Officer) to identify further weaknesses and/or potential threats from cyber to which they may be exposed.

Lloyd's would also like to re-emphasise the importance of having in place an open and transparent culture and encouraging employees to feel comfortable raising concerns. This is likely to encourage employees to more willingly report any potential security incidents, which in turn will prompt more frequent investigation into incidents and lessons learned leading to additional controls being implemented to further strengthen the cyber security framework.

CDM 1.4 Cyber Protection

Managing agents shall ensure that they have protection capabilities in place.

Managing agents shall:

- obtain Cyber Essentials accreditation on an annual basis to reduce the operational risk of common cyber-attacks;
- implement mandatory annual cyber security and data protection training for all staff and have a cyber security and data protection awareness programme in place;
- ensure appropriate security testing takes place on all new systems and any findings are remediated in line with the managing agent's risk appetite; and
- have other appropriate technical and non-technical controls in place to protect it's key services, processes and underlying systems.
-

For this specific area, Lloyd's are building on the previous minimum requirement for an agent to be Cyber Essentials compliant. In addition to the technical control themes within Cyber Essentials, managing agents will also be required to have annual mandatory cyber resilience training in place for all staff and to undertake security testing of all new systems. It is not expected that these will be the only protections that a managing agent has in place.

Cyber Essentials is a UK Government backed scheme (sponsored by the NCSC) that concentrates on five technical 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 based on 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.ncsc.gov.uk/

Cyber security and data protection awareness and training are a key pillar of cyber protection due to a managing agent's staff being part of its cyber defence. At minimum, managing agents should have annual mandatory training in place for all staff, this ensures that there is at least one checkpoint throughout the year where staff receiving training on the threats, risks and their responsibilities around cyber resilience. However, mandatory training is only a small part of effective awareness and managing agents should also have some form of awareness plan of activities throughout the year covering cyber security and data protection.

The building, configuring, implementing or procuring of new systems or applications should be done using the principles of 'security-by-design' and 'privacy-by-design', whether it is built in-house or only configuring a software-as-a-service. Security requirements should be a part of the design and implementation process and a key part of assuring this is through the running of appropriate security testing, such as technical penetration testing, build reviews or application security testing, by competent ethical hackers. For systems built or heavily customised by the managing agent we would expect appropriate security testing to initiated by the managing agent. The findings from such security testing should be remediated in line with the organisation's risk appetite and resolved before the 'Go-Live' of the system in question. For software-as-a-service systems or applications we would expect appropriate security testing to have been performed by the vendors during their design and build phases.

Beyond the minimum cyber protections stipulated above managing agents should also be ensuring that they have other technical and non-technical controls in place to protect their key services, processes, systems and data. These could include but are not limited to:

- Robust identity, authentication and access management controls are in place ensuring that privilege access to systems are more tightly controlled, principles of least privilege and segregation of duties are applied and multi-factor authentication is deployed;
- Ensuring that security requirements are embedded into business process and system design;
- Vulnerability management controls to identify and remediate vulnerability in systems and applications.

CDM 1.5 Cyber Third-Party Management

Managing agents shall establish an approach to enable the management of cyber risks associated with third parties and external suppliers.

Managing agents shall:

- develop a policy and processes for managing cyber risks associated with key suppliers and outsource providers.

Managing agents should have a documented process for managing the cyber resilience risks associated with external suppliers. Ideally this process will be incorporated into the broader procurement led supplier management process and involve inputs from information security, data protection and business continuity teams/functions at key stages.

Typical activities could include:

- Categorising third parties and suppliers in order of importance or risk profile, for example: providers of key business services, processors of sensitive data;
- agreeing security arrangements with third parties and suppliers and assessing their security capabilities, using a risk-based approach;
- assessing changes to the organisation's information risk profile, that may result from the onboarding of a new third parties or suppliers.

CDM 1.6 Cyber Detection

Managing agents shall ensure that they have detection capabilities in place.

Managing agents shall:

- develop and implement appropriate controls to identify the occurrence of a cybersecurity event in a timely manner (e.g. through identifying anomalies and events, implementing security continuous monitoring and detection processes).

Managing agents could develop the ability to detect an intrusion early and take a defence-in-depth approach by instituting multi-layered detection controls covering people, processes, and technology, with each layer serving as a safety net for preceding layers.

An effective intrusion detection capability could also assist a managing agent with identifying deficiencies in their protective measures for early remediation. These capabilities would include data loss/leaks prevention and detection,

the recording and documentation of audit logs, event data aggregation, correlation, analysis and communication, as well as network, personnel and external dependency activity monitoring.

Managing agents could employ monitoring and detection capabilities to facilitate its incident response process and support information collection for the forensic investigation process.

Some organisations are more forward thinking in their approach through the use of more advanced technology and techniques and access to more forward looking KRIs for monitoring (e.g. employee behaviors and patterns) and from this being able to distinguish what 'normal' versus 'anomalous' activity looks like (e.g. individuals attempting to uninstall a particular anti-virus software, disable a firewall or install a new piece of software).

In some cases, responsibility for performing the monitoring/testing has been outsourced to an external third party, with the added benefits of being able to access state of the art technology/more sophisticated monitoring software.

Other organisations deploy so-called 'threat-hunters' to proactively seek out potential threats and vulnerabilities within existing /systems (applications and networks).

It is also essential that monitoring is performed on both incoming (e.g. web, email or USB) traffic and out-going channels to ensure the risk of a successful attack is minimised.

CDM 1.7 Cyber Response and Recovery

Managing agents shall ensure that they have incident response and recovery capabilities in place.

Managing agents shall:

- develop response and communication plans for use in the event of a Cyber Incident, with these plans subject to review and improvement as appropriate;
- have in place plans and procedures to recover from a Cyber Incident, with such recovery arrangements designed to enable managing agents to resume operations safely with a minimum of disruptions to policyholders and business operations;
- test and exercise response and recovery plans and procedures at appropriate intervals.

Managing agents could implement incident response policies and other controls to facilitate effective incident response, these controls should clearly address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders including up to date contact lists.

Recovery of operations that are interrupted by a Cyber Incident should occur once operational stability and integrity are assured. Where critical services, processes and underlying systems have been affected, restoration should be undertaken in accordance with objectives set by the relevant public authorities.

CDM 1.8 Cyber Information Sharing

Managing agents shall ensure that they have a process in place to enable the sharing of cyber risk/resilience information with internal and external stakeholders.

Managing agents shall:

- endeavor to engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders;
- ensure this information covers threats, vulnerabilities, incident response, recovery and lessons learnt; to enhance defences, limit damage caused by successful attacks and broaden awareness and understanding of the cyber threat within their organisations.

Internal stakeholders

Internal stakeholders would typically be employees, consultants and third parties within the managing agent who have an interest in receiving cyber risk/resilience information.

Cyber threat intelligence

When properly contextualised, cyber threat intelligence enables a managing agent to validate and inform the prioritisation of resources, risk mitigation strategies, and training programmes in relation to cyber resilience. Therefore, a managing agent should make cyber threat intelligence available to appropriate staff within the organisation with the responsibility for the mitigation of cyber risks at the strategic, tactical, and operational levels. Cyber threat intelligence should be used to ensure that the implementation of any cybersecurity measures is threat-informed.

External stakeholders

External stakeholders would typically be people who do not work for the managing agent including representatives from strategic partners, peer companies, government and law enforcement agencies.

Market cyber forum

Discussions are currently underway to revive the market cyber forum to enable peers within the Lloyd's market and public authorities to network, share experiences and concerns and to discuss changes in cyber regulation, the evolving cyber risk landscape and threats facing the community.

These activities serve to deepen collective understanding of how attackers may exploit sector-wide vulnerabilities that could potentially disrupt critical economic functions and endanger financial stability, managing agents, the global Lloyd's market and the UK financial services sector will benefit from this collaboration.

It could also serve as a useful forum to discuss and agree the level of communication and dialogue which should / needs to occur between the slip lead and the following market in the event of a cyber-attack. Specifically, what steps would be taken to communicate the incident to the follow managing agents explaining the root cause, break down in controls resulting in the attack, potential impact and details of any controls which have been implemented subsequently.

These meetings would typically be physical with attendees convening in an agreed office location at regular intervals throughout the year.

An online forum for effective collaboration

The Cybersecurity Information Sharing Partnership (CiSP) is another good resource for receiving and sharing threat intelligence with mainly external stakeholders. This is an online collaboration forum, sponsored by the NCSC that enables both sharing and receiving of various types of information (alerts, advisories, case studies etc.) from both UK and international sources.

Sharing technical information via the CiSP, such as threat indicators or details on how vulnerabilities were exploited, allows organisations to remain up-to-date in their defences and learn about emerging modes of operation used by attackers.

The CiSP also enables participants to create their own private ‘special interest’ groups and/or to join existing public groups.

For more information, visit: www.ncsc/cisp

Section 2: Data Management

The Data Management standards here cover both data in general and also internal model data as covered in MS13 Modelling Design and Implementation. Additional specific requirements on internal model data can be found in MS13 Section 6.

CDM 2.1 Data Protection

Managing agents shall comply with all data protection regulations and guidance issued by the data protection authority or regulator for the jurisdiction(s) in which they process personal data.

Managing agents shall:

- notwithstanding any requirement to report a Personal Data Breach to comply with any law or regulation, managing agents shall report Personal Data Breaches to Lloyd's via their designated Oversight Manager as soon as possible after they become aware of the same and within 72 hours at the latest; and
- following reporting, managing agents shall engage in constructive discussions with their designated Oversight Manager on the Personal Data Breach, and take such steps as are reasonable both to mitigate the effects of the Personal Data Breach and to reduce the chances of its reoccurrence..

Managing agents will be aware that the processing of personal data is regulated in the UK by the Data Protection Act 2018, which incorporates GDPR (including in Section 207 of the Data Protection Act 2018, the extra-territorial elements) and the Privacy and Electronic Communications Regulations. Equivalent or analogous data protection regulations are likely to apply in territories in which managing agents may operate or process personal data.

In the UK and in other territories where the GDPR applies, managing agents must ensure that all processing of personal data complies with the Principles set out in Article 5 GDPR and all personal data is processed lawfully as set out in Article 6 GDPR.

A concern of Lloyd's is to ensure that its Oversight Managers are aware of all Personal Data Breaches that may affect the Lloyd's market, whether they have to report them to other regulators or not. This is of concern to Lloyd's itself, and because others in the market could be affected by the same or a similar Personal Data Breach. As such, there is a requirement for managing agents to:

- report all Personal Data Breaches to their designated Oversight Manager as soon as they become aware of the same; and
- engage in constructive discussions with their Oversight Manager and take such steps as are reasonable both to mitigate the effects of the Personal Data Breach and to reduce the chances of its reoccurrence.

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

CDM 2.2 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, including internal model data;
- have an appropriate policy (or policies) covering the overarching requirements for how data, including internal model data, must be governed;
- have appropriate policies and procedures in place to allow timely recording and production of data, including internal model 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, including internal model data, to the Board, relevant committees and Lloyd's; and
- ensure that roles and responsibilities for the management of data, including internal model 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 functions, 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 set the tone and provide appropriate oversight of the implementation of data policy or policies with regards to data, including internal model data, necessary for business purposes, regulatory reasons and/or sound decision making. The data governance framework should set principles for the governance and overall management of data including but not limited to: data as an asset, retention, quality, compliance with statutory/legal/regulatory requirements, protection of data, ownership and senior accountability. 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. The data governance framework should also ensure that data is appropriate, accurate, complete and timely reported where they relate to data returns in order to support required governance and management decision making processes, together with prompt detection of issues.

Managing agents should also ensure that the necessary MI is produced for regular reporting to the Board, relevant committees and Lloyd's. This should include MI to determine whether the syndicate is meeting strategic plans, Syndicate Business Plans, budgets, forecasts and other model uses, such as operating within risk appetite.

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.

CDM 2.3 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, including internal model data, which is sufficient in granularity and coverage to enable the actuarial function(s) to appropriately monitor experience and perform forecasting;
- to record data, including internal model data, which is sufficient in granularity and coverage to monitor performance against Syndicate Business Plans and forecasts;
- with relevant data from models and forecasts built into the data infrastructure for the production of internal model data returns to Lloyd's.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 MI 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 regards 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.

CDM 2.4 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 all 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, MI 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 have been and will continue to be given in advance. Further information on specific impacted returns and timelines continue to be published 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 MI 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.

APPENDIX – LINKS

- Data Protection Act 2018 –

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

- GDPR –

  https://gdpr.eu/

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

  https://www.lloyds.com/mdc