LLOYD'S

Principles for doing business at Lloyd's

Summary of revisions for 2024

LLOYD'S

Principle 1: Underwriting Profitability

Updates for 2024

Summary of the change: The wording in sub-principle 8 of the Underwriting Profitability Principle has been revised. To reduce ambiguity, we have amended references to ESG to either "sustainability" or more specifically to "environmental and social risks". This aligns with our recently published Insuring the transition roadmap consultation.

Amended content in blue text.

UNDERWRITING PROFITABILITY

8 **Have processes in place to support decision making in relation to ~~ESG integration~~ integrating sustainability into underwriting.**

Foundational	Intermediate	Established	Advanced
• Board approved Sustainability ~~ESG~~ Strategy covers approach to sustainable underwriting. • Sustainability ~~ESG~~ Strategy focuses on the most material areas of sustainable underwriting operations and how Sustainability ~~ESG~~ can be integrated into these areas. • Underwriting Governance Framework is aligned with broader Sustainability ~~ESG~~ governance. • Data requirements needed to aid decision making have been identified and efforts are underway to gather the necessary data to understand, monitor and report on environmental and social ~~ESG~~ exposures.	• Board approved Sustainability ~~ESG~~ Strategy and approach to sustainable underwriting is cascaded throughout the managing agent through sustainability ~~ESG~~ targets. • Analysis of existing portfolios carried out to identify incumbent exposures/client relationships that may not be supportable going forward based on syndicates' Sustainability ~~ESG~~ Strategy.	• Board approved Sustainability ~~ESG~~ strategy fully embedded and aligned with overall underwriting strategy, annual business plan process and risk appetites. • Additional qualitative Sustainability ~~ESG~~ considerations are included as part of business planning. • Full awareness of which exposures in existing portfolio are not aligned with syndicates' sustainable insurances framework; either elected to non-renew or are working with the insured and supporting their transition.	• Additional focus on Sustainability ~~ESG~~ and product innovation through new business. • Written guidance is provided articulating Sustainability ~~ESG~~ approach alongside any delegated authority. • Protocol for examining data through established systems. • Granularity of data used is appropriate for the needs and business profile. • Pricing underwriting systems in place to review whether assumptions / data are appropriate from a sustainability perspective. • Policyholder engagement strategy established. • Work underway to develop credible transition plans with policyholders which pose the most material environmental and social ~~ESG~~ risks based on syndicates' Sustainability ~~ESG~~ strategy.

Principle 1: Legacy Reinsurance Underwriting Profitability

(RITC syndicates only)

Summary of the change: As part of Lloyd's wider oversight enhancements for the legacy reinsurance market, we have introduced an adapted Legacy Reinsurance Underwriting Profitability Principle. This will enable us to assess capability across strategy, pricing, ongoing performance including expense management, and governance. We communicated this change to relevant syndicates in market workshops during 2023. This will apply to RITC syndicates only and should be attested to in March 2024 as part of the Principles Board Attestation.

The full Principle and guidance can be found in the main Principles document.

Managing agents should ensure their strategy for underwriting legacy reinsurance transactions is clear and that pricing assumptions are sufficiently robust, to ensure the sustainable run-off of acquired liabilities.

To support this, managing agents should ensure their syndicates:

1	Have a clear and robust medium to long term business strategy with clearly defined and understood underwriting risk appetite, giving consideration to existing legacy reinsurance transactions on the balance sheet
2	Develop and execute legacy business plans which align with their business strategy
3	Not applicable
4	Manage and control expenses in order to ensure they are appropriate for the business written
5	Not applicable
6	Have an effective pricing framework in place in order to set sustainable pricing for legacy transactions that will ensure the discharge of assumed liabilities within the assets received with, and generated by, the assumed portfolio
7	Have robust governance processes in place to support legacy underwriting decision making, with underwriting assumptions clearly articulated and understood by stakeholders supported by proactive involvement and sufficient challenge by the wider functions
8	Not applicable

Sub-principle numbering follows the Underwriting Profitability Principle

Legacy Reinsurance Underwriting Profitability

Managing agents should ensure their strategy for underwriting legacy reinsurance transactions is clear and that pricing assumptions are sufficiently robust, to ensure the sustainable run-off of acquired liabilities.

LEGACY REINSURANCE UNDERWRITING PROFITABILITY

1 Have a clear and robust medium to long term business strategy with clearly defined and understood underwriting risk appetite, giving consideration to existing legacy reinsurance transactions on the balance sheet

	Foundational	Established	Advanced
Strategy	• Underwriting strategy is set collaboratively with engagement and feedback loops between the relevant stakeholders	• Underwriting strategy outlines a forward-looking plan concerning the key elements that identify a target contract	• Regular horizon scanning towards emerging risks is considered and reflected within the underwriting strategy
Risk Appetite	• The board has defined underwriting risk appetite statements. These are linked to and contained within the syndicate business plan • Risk appetite statements reflect market level feedback from Lloyd's and regulatory concerns	• Performance assessment for senior management considers adherence to risk appetite	• Underwriting strategy is forward looking, allowing agile management of the due diligence process employed in underwriting

LEGACY REINSURANCE UNDERWRITING PROFITABILITY

2 **Develop and execute legacy business plans which align with their business strategy.**

Business Planning

Foundational	Established	Advanced
• Business plan aligns with the syndicate's medium to long term underwriting strategy and risk appetite • Business plan is kept under review, with KPIs monitored and reported to the board at an appropriate frequency • Timely actions are taken to address variances to business plan, and root cause analysis conducted to fully understand underlying drivers • The underlying drivers are fed back into the due diligence process for future underwriting	• Monitoring allows for identification of both positive and adverse variation to plan • Suite of KPIs are kept under review to consider if any changes are required to the metrics themselves or any additions to ensure early detection of issues • Regular review of business plan and KPIs incorporates latest analysis from other functions and promotes consistency	• Thematic findings are drawn out from underwriting operational KPI monitoring. These are fed back into the due diligence process for future underwriting with training in place to address gaps

LEGACY REINSURANCE UNDERWRITING PROFITABILITY

4 **Manage and control expenses in order to ensure they are appropriate for the business written.**

Expense Management

Foundational	Established	Advanced
• Medium to long term strategy in place to control overall net operating expense • Internal expense policy in place with appropriate thresholds and referral points • Quarterly data and MI in place to track position against expected and action taken to remediate where required • Administration expenses are proportionate and are forecast in line with planned underwriting strategy	• Monthly data and MI in place to track position against expected and action taken to remediate where required • Forward looking identification of potential expenses necessary to support strategic decision making. Proactive action taken to manage expenses over medium to longer term • All aspects of operational expenditure are understood and considered as part of the syndicate's underwriting strategy	• Real time tracking in place to assess the position of operating expenses against expected with proactive measures adopted to address actual and forecast variance

LEGACY REINSURANCE UNDERWRITING PROFITABILITY

6 **Have an effective pricing framework in place in order to set sustainable pricing for legacy transactions that will ensure the discharge of assumed liabilities within the assets received with, and generated by, the assumed portfolio**

Pricing

Foundational	Established	Advanced
• Experience based pricing approach is used • Pricing policy and procedure have been reviewed and approved by the board and are fully documented • Pricing decisions and rationales are captured and analysed on an ongoing basis for adjustments based on the outturn of the acquired business • Pricing policy and procedure are reviewed regularly to ensure that they are up to date with the current experience of the syndicate • The parameters employed in the due diligence process for underwriting are consistent with, and support, the syndicate's business plan • Resourcing is adequate to conduct due diligence to a standard that results in viable pricing of all the transactions being pursued by the syndicate	• Resourcing allows for more in-depth analysis feeding into the pricing process, with forward looking views feeding into assumptions • The view of risk is incorporated into pricing at syndicate level, such as the impact of concentration risk of the target portfolio on the existing portfolio. This is done on a forward-looking basis	• *No incremental guidance, Lloyd's will consult to further develop our view*

LEGACY REINSURANCE UNDERWRITING PROFITABILITY

7 **Have robust governance processes in place to support legacy underwriting decision making, with underwriting assumptions clearly articulated and understood by stakeholders supported by proactive involvement and sufficient challenge by the wider functions.**

Governance

Foundational	Established	Advanced
• Underwriting governance framework is in place with reporting lines and committee framework defined • No binding bid is made unless approved by the appropriate committee which includes Independent Non-executive Directors to ensure that it is consistent with the internal rate of return set out in the syndicate's business plan • Any bid put before the appropriate committee is sufficiently detailed to allow that committee's participants to ensure that the assumptions used are in line with the syndicate's business plan and reasonable market expectations • A process is in place to document whether due diligence has followed the approved process and that document is available to the transaction approving committee	• The senior management have established a culture of accountability at all levels of the syndicate, including clear risk control expectations and a no blame culture for reporting underwriting issues	• The board and senior management actively promote challenge to underwriting including the parameters and assumptions used

Principle 2: Catastrophe Exposure

Updates for 2024

Summary of the change: The structure of the Catastrophe Exposure Principle (applies to Nat Cat and Non Nat Cat) has been revised to align the information required from managing agents directly with Lloyd's review approach. For 2024, we have converted the 10 previous "components" of the 5 sub-principles into a new set of 10 sub-principles (applies equally to Nat Cat and Non-Nat Cat). The sub-principle wordings have been revised for clarity but there is no change to the Principle wording or underlying guidance.

Previous Sub-Principles	Previous Components	New sub-principles for 2024
1) Manage catastrophe exposure in line with agreed cat risk appetites	Risk Appetite	1) Manage catastrophe exposure in line with their agreed risk appetites and tolerances.
2) Employ data standards, risk quantification tools, controls, expertise, and reporting frameworks which are appropriate to their risk profile	Data and Tools	2) Employ appropriate tools to support effective and efficient exposure data capture, management and use.
	Exposure Monitoring and Reporting	3) Adopt a robust risk-based framework for exposure quantification and monitoring, to support downstream decision making
	Resourcing	4) Have the teams and expertise in place to meet the business needs, including strategic projects, regular deliverables and research and development
3) Adequately justify and validate methodology and assumptions, including expert judgements	Model methodology	5) Define and maintain an appropriate cat view of risk methodology
	Model Validation	6) Implement appropriate risk-based validation of the cat view of risk
4) Representation of catastrophe risk, in the internal model, is complete, reflects all possible sources of loss and is used effectively by wider business functions	Model completeness	7) Maintain a materially complete representation of cat in the syndicate view of risk
	Model Change	8) Adopt a robust risk-based framework for managing changes to cat view of risk and exposure management methodologies
	Model use and capital modelling	9) Maintain consistent understanding, use and continual development of cat view of risk outputs
5) Have robust governance and oversight of risk aggregations	Governance and oversight	10) Have robust governance and oversight of risk aggregations

Principle 12: Operational Resilience

Updates for 2024

Summary of the change: The Operational Resilience Principle has been revised, with the introduction of four levels of expected maturity (previously all managing agents expected maturity was Foundational) and revised sub-principle wording and guidance.

Principle (unchanged):

Managing agents should maintain robust and resilient operations, embedding cyber resilience and effective third-party risk management.

Previous Sub-Principles	New sub-principles for 2024
1) Prioritise resilience of the most important services; embedding appropriate governance for operational resilience into their businesses and prioritising recovery of Important Business Services within identified and tested impact tolerances.	1) Operate a robust operational resilience framework
2) Invest in their operational resilience, including their control environments, so that the risk of a future event causing harm to customers or threatening the managing agent's viability is mitigated	2) Maintain oversight of operational resilience through appropriate governance processes and risk and control environments
3) Embed cyber resilience into operations: Managing agents must protect their information systems, processes, people and data from external or internal compromise to prevent harm to customers, loss of data, contagion and/or reputational damage to the wider Lloyd's market.	3) Maintain appropriate cyber resilience

Given the extensive updates to the guidance within the maturity matrix and the addition of new levels of expected maturity, a comparison or mapping is not provided. However, the following slides contain the previous guidance for comparison against the revised Principles document

Principle 12: Operational Resilience

Managing agents should maintain robust and resilient operations, embedding cyber resilience and effective third-party risk management.

OPERATIONAL RESILIENCE

1 Prioritise resilience of the most important services; embedding appropriate governance for operational resilience into their businesses and prioritising recovery of Important Business Services within identified and tested impact tolerances.

Foundational	Established	Advanced
• Managing agents can evidence a roadmap for embedding operational resilience into the business within regulatory timelines • A system of governance and reporting to the board is in place to monitor managing agents' operational resilience. • Self-assessment documented for all Important Business Services of the business, and approved by board by 31 Mar 2022 and annually thereafter or when there is a material change to an Important Business Service. • Severe but plausible scenarios identified, recovery plans and workarounds are in place • Managing agents can evidence an approach for mapping that gives the business a reasonable level of confidence that all critical resources are identified • Managing agents have developed policy and processes for managing risks associated with key suppliers and outsource providers, and consider substitution	• Identified Important Business Services and tested that they can recover within impact tolerances • Scenario libraries consider contagion in testing the impact on multiple Important Business Services • Managing agents can evidence an approach for mapping that gives the business a granular level of detail that all critical resources are identified	• *No incremental guidance*

Principles

2 **Invest in their operational resilience, including their control environments, so that the risk of a future event causing harm to customers or threatening the managing agent's viability is mitigated.**

Foundational	Established	Advanced
• Managing agents learn lessons from incidents and tests. • Managing agents prioritise lessons learned in their investment plans.	• Managing agents can evidence prioritisation of their change programmes to embed operational resilience by design within their Important Business Services • Participate in market wide scenario exercises and invest in vulnerabilities • Managing agents evidence a wider range of testing approaches embedded into their businesses to identify vulnerabilities	• *No incremental guidance*

Principles

3 **Embed cyber resilience into operations: Managing agents must protect their information systems, processes, people and data from external or internal compromise to prevent harm to customers, loss of data, contagion and/or reputational damage to the wider Lloyd's market.**

	Foundational	Established	Advanced
Cyber Information Systems & Reporting	• 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, Material Cyber incidents must be reported to Lloyd's via their designated Account Manager as soon as they become aware of the same • Following reporting, managing agents shall engage in constructive discussions with their designated Account 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.	• *No incremental guidance*	• Information systems should be fully documented and set out which information is to be shared, by whom, and when. Documentation allows for information to flow up and down hierarchy levels as well as horizontally between different business units where appropriate. • Demonstrate there is clear understanding of how all information systems are linked, with controls addressing data integrity issues. • There is clarity and transparency over staff access to information systems for providing input from and to their areas of responsibility. In addition, there is clarity on who the relevant personnel are that need to have passive access to the system as to retrieve data for the proper discharge of their duties.
Data Protection and Governance	• Notwithstanding any regulatory requirement to report a Personal Data Breach, Personal Data Breaches must be reported to Lloyd's via the designated Account Manager as soon as they become aware of the same and within 72 hours at the latest. • Engage in constructive discussions with the Lloyd's Account Manager on Personal Data Breaches and take reasonable steps to mitigate effects and reduce chances of a reoccurrence. • Director in place with accountability for oversight of the data governance framework with an appropriate data governance policy in place. • Clear roles and responsibilities are in place for data management. • Appropriate policies and procedures in place to allow timely recording and production of data to ensure data returns are appropriate, accurate, complete and submitted on time.	• *No incremental guidance*	• *No incremental guidance*

Principles

3 **Embed cyber resilience into operations: Managing agents must protect their information systems, processes, people and data from external or internal compromise to prevent harm to customers, loss of data, contagion and/or reputational damage to the wider Lloyd's market.**

Cyber Governance & Identification

Foundational	Established	Advanced
• 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 cybersecurity framework and sets the tolerance for cyber risk • Conduct regular reviews of cyber resilience capability to highlight any material gaps and/or areas for improvement • 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. • Taking a risk-based approach in identifying those services, processes and underlying systems (networks, applications and data) that are critical • Assessment of the current internal and external threats, followed by determination of the likelihood and impact of a cyber compromise or data breach on those critical services, and then development of a set of holistic controls in a proportionate and cost-effective way.	• *No incremental guidance*	• 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 business) • Conduct regular reviews, at least annually, of the cybersecurity framework against industry standards to highlight any material gaps/areas for improvement and to use the output to formulate the IT strategic plan • Assurance activities are visibly joined up across the three lines of defence • 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 forums responsible for oversight of cyber.

Principles

3 **Embed cyber resilience into operations: Managing agents must protect their information systems, processes, people and data from external or internal compromise to prevent harm to customers, loss of data, contagion and/or reputational damage to the wider Lloyd's market.**

Cyber Protection

Foundational	Established	Advanced

• Obtain Cyber Essentials accreditation on an annual basis to reduce the operational risk of common cyber-attacks
• Implement regulatory mandatory cyber security and data protection training, at least annually, 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 risk appetite
• Have other appropriate technic al and non-technical controls in place to protect key services, processes and underlying systems
	• *No incremental guidance*	• Obtain Cyber Essentials Plus accreditation which offers a higher level of assurance through the external testing of the cyber security approach. Findings from such security testing are remediated in line with risk appetite and resolved before the 'Go-Live' of the system in question.
		• Comprehensive technical and non-technical controls are in place to protect their all services, processes, systems and data. These could include but are not limited to:
		  • Robust identity, authentication and access management controls to ensure 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
		  • Security requirements are embedded into business process and system design
		  • Vulnerability management controls to identify and remediate vulnerability in systems and applications.

Principles

3 **Embed cyber resilience into operations: Managing agents must protect their information systems, processes, people and data from external or internal compromise to prevent harm to customers, loss of data, contagion and/or reputational damage to the wider Lloyd's market.**

	Foundational	Established	Advanced

Cyber third-party management	• Policy and processes in place for managing cyber risks associated with key suppliers, outsource providers, coverholders and TPAs.	• *No incremental guidance*	• Documented process for managing the cyber resilience risks associated with all external suppliers which is incorporated into the broader procurement led supplier management process and involves 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 information risk profile, that may result from the onboarding of a new third parties or suppliers.

Cyber detection	• 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). • 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.	• *No incremental guidance*	• 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. • Monitoring and detection capabilities in place to facilitate its incident response process and support information collection for the forensic investigation process.

Principles

3 **Embed cyber resilience into operations: Managing agents must protect their information systems, processes, people and data from external or internal compromise to prevent harm to customers, loss of data, contagion and/or reputational damage to the wider Lloyd's market.**

	Foundational	Established	Advanced
Cyber response and recovery	• Response and communication plans for use in the event of a Cyber Incident, with these plans subject to review and improvement as appropriate • Plans and procedures in place to recover from a Cyber Incident, with such recovery arrangements designed to enable that operations are safely resumed with a minimum of disruptions to policyholders and business operations • Test and exercise response and recovery plans and procedures at appropriate intervals.	• *No incremental guidance*	• *No incremental guidance*
Cyber information sharing	• Engage in the timely sharing of reliable, actionable cybersecurity information (which could include threats, vulnerabilities, incident response, recovery and lessons learnt) with internal and external stakeholders • Attacks and threat intelligence are used to broaden understanding of the cyber threat within the business.	• *No incremental guidance*	• Active members of the LMA CISO Community and potentially have a seat at the CISO committee. • Intelligence from threats, incidents and breaches is actively shared with Lloyd's and across the population of other managing agents (in a secure way) potentially via the LMA CISO Community.