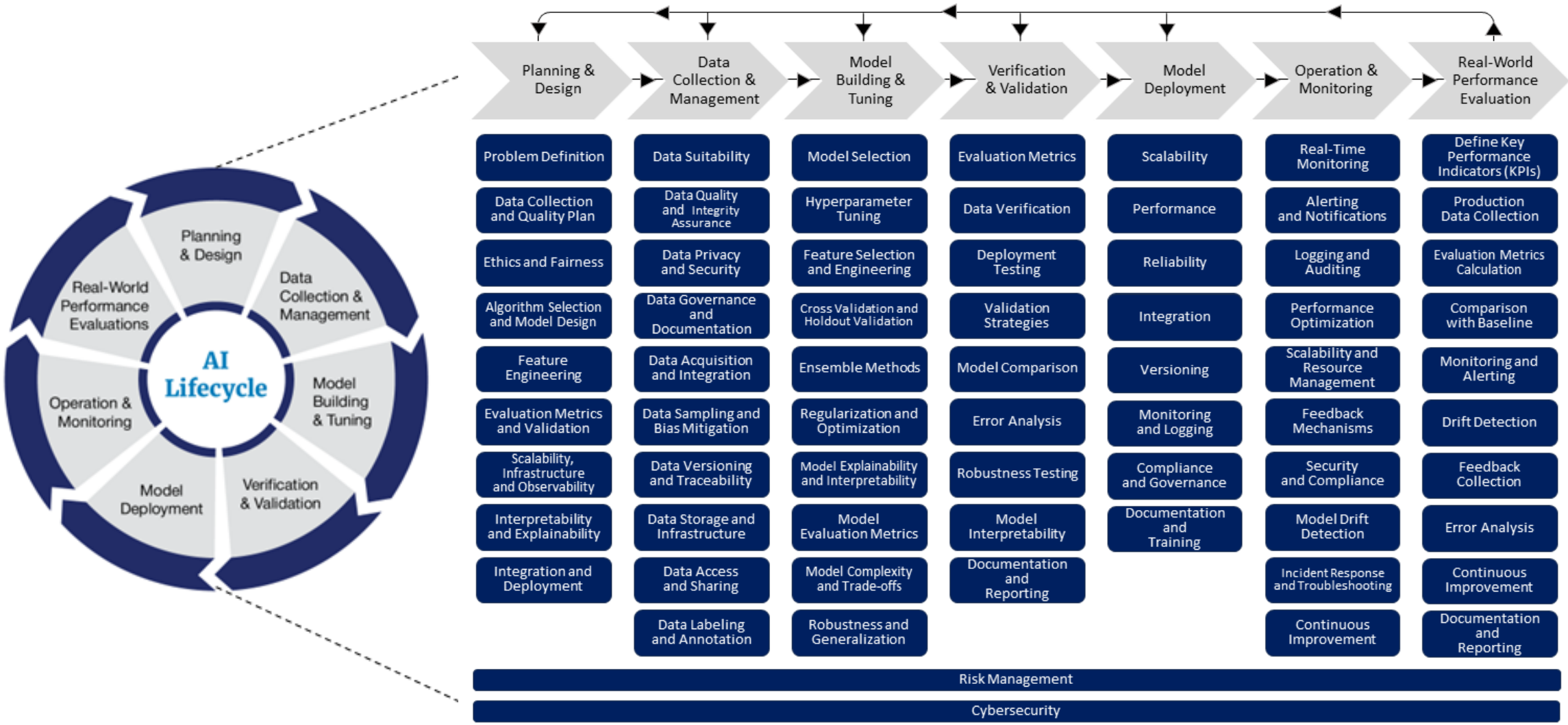
The AI Lifecycle expanded to illustrate per-phase considerations



Text Explanation of Illustration

The illustration shows the AI lifecycle management wheel to the left expanded on the right to include further details of the lifecycle phases. The chevrons shown there represent the lifecycle phases: namely planning and design, data collection and management, model building and tuning, verification and validation, model deployment, operations and monitoring, and real-world performance evaluation. Each chevron is shown with a stack of candidate technical and procedural considerations to be addressed in each lifecycle phase.

Specifically, the planning and design lifecycle phase includes the following considerations: problem definition, data collection and quality plan, ethics and fairness, algorithm selection and model design, feature engineering, evaluation metrics and validation, scalability infrastructure and observability, interpretability and explainability, and integration and deployment.

The data collection and management lifecycle phase includes the following considerations: data suitability, data quality and integrity insurance, data privacy and security, data governance and documentation, data sampling and bias mitigation, data versioning and traceability, data storage and infrastructure, data access and sharing, and data labeling and annotation.

The model building and tuning lifecycle phase includes the following considerations: model selection, hyperparameter tuning, feature selection and engineering, cross validation and holdout validation, ensemble methods, regularization and optimization, model explainability and interpretability, model evaluation metrics, model complexity and trade-offs, and robustness and generalization.

The verification and validation lifecycle phase includes the following considerations: evaluation metrics, data verification, deployment testing, validation strategies, model comparison, error analysis, robustness training, model interpretability, and documentation and reporting.

The model deployment lifecycle phase includes the following considerations: scalability, performance, reliability, integration, versioning, monitoring and logging, compliance and governance, documentation and training.

The operations and monitoring lifecycle phase includes the following considerations: real-time monitoring, alerting and notifications, logging and auditing, performance optimization, scalability and resource management, feedback mechanisms, security and compliance, model drift detection, incident response and troubleshooting, and continuous improvement.

The real-world performance evaluation lifecycle phase includes the following considerations: define key performance indicators or KPIs, production data collection, evaluation metrics calculation, comparison with baseline, monitoring and alerting, drift detection, feedback collection, error analysis, continuous improvement, documentation and reporting.

Risk Management and Cybersecurity are considerations that are shown to apply to each of the lifecycle phases.