

ASSURANCE

MaxIron assurance summary

Public evidence and engagement-specific review

Published assurance position

The MaxIron Trust Centre holds the supplier-assurance position for IBM Maximo services and MaxIron Cloud. It publishes certificate and register links, operational controls, shared responsibilities, possible processing locations and the evidence request route.

ISO/IEC 27001:2022 covers the information security management system and ISO 9001:2015 covers quality management under ISOQAR certificate 27274. The published Cyber Essentials certificate is linked from the Trust Centre. The certificate and scope supplied for formal review determine the current certification position.

Partner and procurement evidence

The IBM Partner Plus directory lists MaxIron as an IBM Gold Partner with Maximo Application Suite proficiency and relevant partner roles. The Digital Marketplace lists MaxIron Ltd as supplier 721548 on G-Cloud 14.

These links support partner and procurement review. An engagement's service scope, security requirements, commercial terms and route to award require the customer's own assessment against the applicable framework and contract.

Operational controls

Published controls include named accounts, multi-factor authentication for human access, least privilege and semi-annual access review. Workforce endpoints use Microsoft Intune, disk encryption, endpoint detection and response, patch compliance and remote wipe.

Provider-native detection and audit logging apply to managed environments. The published cloud audit-retention period is 12 months. Incident response, change management and production restore testing are documented control domains. P1 acknowledgement and resolution figures are targets; coverage and recovery objectives belong to the agreed service schedule.

MaxIron assurance summary

Shared responsibility

MaxIron configures and operates the contracted customer layers. The customer approves business access, data ownership, region, continuity priorities and acceptance. The cloud provider holds responsibilities for the underlying infrastructure under its service terms.

Provider, processing region, network boundaries, backup retention, recovery objectives, maintenance windows and support coverage are agreed for each estate. The public list of possible regions and providers is assessed alongside the engagement's DPA and sub-processor schedule.

Evidence for review

Public material includes policy pages, register links and this summary. The security assurance pack provides the applicable certificate and scope, selected control policies and records, sub-processor position and answers to a named reviewer's questions.

The Statement of Applicability and restricted ISMS evidence are shared under NDA. Architecture, recovery records and data-processing terms are supplied in proportion to the services and risk under review. This summary provides context for due diligence; the formal evidence pack and contract contain the applicable commitments.

Request route

Email security@maxiron.com with the questionnaire or control framework, services and environments in scope, data categories, NDA status and decision date. The same address handles coordinated vulnerability disclosure.

The published policy pages include privacy, cookies, anti-bribery and corruption, and social value. Review them together with the Trust Centre and the service schedule for the proposed engagement.

Full detail and related information

<https://maxiron.com/security/>

Contact: maxiron.com/contact