Credit Benchmark Security Overview

October 2025

Executive Summary

At Credit Benchmark, we recognize that trust is earned—and that data security, operational resilience, and regulatory integrity are foundational to that trust. Our clients operate in some of the most highly regulated and risk-sensitive sectors in the world. As such, we have built and continually refine a security-first culture across every layer of our organization: from infrastructure and product development to governance and incident response.

Because protecting customer data and ensuring the integrity of our analytics is central to our mission, Credit Benchmark employs advanced security and privacy measures across its technology and operations.

The intended audience for this document includes security, compliance, risk management, and information technology (IT) professionals, as well as financial services leaders, who wish to learn more about Credit Benchmark's security posture, including details on technical, operational, and organizational controls.

The goal of this document is to help customers understand primary considerations in all the following areas:

Product Security

Credit Benchmark has designed and built security into its agile software development life cycle by automating security checks in the development pipeline and training every developer on secure coding practices. Additionally, Credit Benchmark's products have controls in place for identity and access management, data protection, and backup.

Operational Security

Credit Benchmark maintains an active posture regarding threat detection, incident management, disaster

recovery and business continuity plans.

Organizational Security

Credit Benchmark's dedicated security and privacy programs are externally audited annually. The company

maintains an ISO 27001 certification (international standard for information security) and a SOC 2 Type 2 attestation (covering security and the Trust Services Criteria). In addition, Credit Benchmark aligns its security program and capabilities with the National Institute of Standards and Technology (NIST) Cloud Computing Standards, Open Web Application Security Project (OWASP) and Center for Information Security (CIS).

Privacy

Credit Benchmark complies with all applicable data protection laws in its provision of services, including the

General Data Protection Regulation (GDPR) and maintains a Privacy Policy which Is updated on an annual basis.

Product Security

Infrastructure Security and Engineering

Credit Benchmark leverages leading service providers with industry-recognized certifications such as ISO 27001, SOC 1, and SOC 2. This enables us to scale securely, maintain system resilience, and safeguard the confidentiality, integrity and availability of client data. Credit Benchmark's use of on-premise and cloud service providers enables the company to quickly iterate and test the quality, performance, and security of its systems — and to maintain control over the security of data, systems, and services within its computing environments. Credit Benchmark achieves this through measures

such as infrastructure configuration automation, vulnerability management, data and system backups, and pre-emptive threat detection. A variety of network security controls, including network segmentation, firewalls, and traffic monitoring, are enforced within the production compute environments. In order to safeguard data from external threats, production, development and test compute environments are isolated from each other and the company's corporate enterprise networks.

Security checks are embedded in key phases of the infrastructure engineering lifecycle. Furthermore, all code written by the company's infrastructure engineers is required to be reviewed, approved, and tested prior to release, to ensure it adheres to the highest quality, performance, and security standards.

Credit Benchmark's infrastructure is annually subjected to a wide range of different penetration tests, business continuity test, disaster recovery capability tests, and external audits. Credit Benchmark's infrastructure is hardened based on security goals, National Institutes of Standards and Technology (NIST) standards, and Center for

Internet Security (CIS) controls.

Software Development Life Cycle

Credit Benchmark's software engineering organization follows a standardized software development life cycle (SDLC), embedding security at key phases. All software engineers are regularly trained on secure coding practices, ensuring that software development is both efficient and secure. The company practices security-by-design principles by incorporating threat modelling and security architecture reviews for key releases and systems. Software and security teams perform multiple rounds of rigorous review during the design phase of all major features. Any changes to the code base require additional testing, review, and approval prior to migration to production. Security tooling is integrated into Credit Benchmark's code pipeline, which incorporates a number of checks for application security vulnerabilities (including but not limited to the latest OWASP Top 10 risks), such as static code analysis, and dependency checking. In addition, members of the security team perform manual application security testing on key components. Any vulnerabilities discovered via automated or manual means are routed through the software engineering work tracking system, and are governed by internal SLAs to ensure timely remediation and significantly reduce the risk

exposure window.

Identity and Access Management

Within Credit Benchmark's solutions individuals can be configured with fine-grained access controls and user roles to align with organizational policies. Integration with enterprise single sign-on (SSO) and multi-factor authentication (MFA) ensures that only authorized individuals gain access. Additional safeguards such as IP whitelisting and API integrations can be utilised to extend protection.

All key actions — such as data updates, report generation, and configuration changes — are logged with user attribution, time stamps, and audit records, ensuring traceability and accountability.

Data Protection and Backup

Credit Benchmark ensures the confidentiality, integrity, and availability of customer data. Data is encrypted in transit (TLS 1.2+) and at rest (AES-256). Customer data is stored in secure, geographically redundant environments within the UK and Ireland.

High-redundancy storage systems minimize the risk of data loss. Structured data and derived analytics are backed up daily, supporting robust recovery and compliance with financial industry standards.

Credit Benchmark maintains a robust data retention and backup strategy designed to support operational resilience, regulatory compliance, and customer trust. All client data is retained for the duration of the customer relationship, ensuring consistency and continuity across services.

To safeguard against data loss and enable reliable restoration, regular system backups are performed and securely stored. These backups are managed in accordance with industry best practices

Operational Security

Threat Detection

Our monitoring systems use advanced analytics and alerting to identify anomalous activity and potential threats in real time. Vendor-supplied alerts are supplemented by proprietary detection models, continuously refined based on penetration testing and industry intelligence.

Incident Response

While preventative measures remain an essential part of Credit Benchmark's overall strategy for diminishing

security incidents, Credit Benchmark maintains a dedicated security incident response team, which works to minimize the impact of security events in near real-time, and leverages information obtained during each investigation to further strengthen Credit Benchmark's security posture. During an attack, the incident response team proceeds through the phases of Credit Benchmark's security incident response process and plan (IRP), which was created in alignment with industry best practices. The company ensures its readiness for an effective incident response by practicing and educating all internal teams on the correct tools and processes. Periodic tabletop exercises, utilizing real world attack scenarios, are conducted with engineers and business leaders, enabling them to rehearse and fine-tune their responses. Key teams and individuals across the organization have been trained and armed with the right tools to contain, eradicate, and recover from an incident. Furthermore, senior leaders have defined roles and responsibilities in the IRP and receive specific training annually.

Disaster Recovery and Business Continuity Planning

Credit Benchmark maintains a thorough disaster recovery plan, as well as a business continuity plan. Annual testing ensures the company is prepared for black-swan events and can continue to meet all customer commitments — including availability and performance SLAs, recovery time objectives (RTO), and recovery point objectives (RPO).

Credit Benchmark designs its products and services to remain resilient and effective under threat, understanding that external challenges are frequently unpredictable. The company's enterprise IT services and business workflows have also been planned and architected with these customer commitments in mind, so customers' data is always safe.

Organizational Security

Enterprise Security

Credit Benchmark maintains ISO 27001 and 27017 certifications as well as a SOC 2 Type 2 attestation. Credit Benchmark aligns its security program and capabilities with the National Institute of Standards and Technology (NIST)

Cloud Computing Standards, Open Web Application Security Project (OWASP) and Center for

Information Security (CIS). The company's IT services are compartmentalized to limit the security risk of any single component of the system. Credit Benchmark regularly tests, reviews, and monitors its workflows, building detection and defense-in-depth into each of its IT services. Credit Benchmark practices a Zero Trust policy. This means multiple security attributes are assigned to each Credit Benchmark team member and user account, and multi-factor authentication is required in order to access any of the company's IT services. Corporate compliance and security teams maintain procedures to ensure that suppliers are reviewed and assessed for their quality and security, and that each supplier and external service receives careful oversight. The compliance and enterprise security teams conduct assessments, periodic reviews, and audits on vendors, suppliers and contractors whose services may impact product or process quality. In addition, Credit Benchmark undergoes annual security, privacy, and compliance audits by accredited external organizations — covering not only its products and customer-facing services, but also its enterprise security and IT services.

Security Training

All Credit Benchmark employees undergo security training as part of the orientation process and receive ongoing security training yearly throughout their Credit Benchmark tenure. This training is focused on security and privacy policies, procedures, and best practices. This training contains interactive components, such as modules on phishing, malware, and social engineering — requiring team members to engage with the material and demonstrate their understanding of potential threats. Depending on an employee's role, they may be required to undergo additional annual training on specific aspects of security, such as secure coding (in the case of software engineers).

Security Team

Credit Benchmark maintains a dedicated internal security team of security engineers, compliance experts, data engineers, and incident-response professionals. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure, and implementing Credit Benchmark's security policies. The team actively engages with the wider financial security community to maintain best-in-class practices.

Privacy Program

A dedicated security, privacy and legal team jointly manages credit Benchmark's privacy program. These experts ensure that the company's products reflect best-practice privacy standards and adhere to the latest privacy regulations in all applicable countries and states. Credit Benchmark complies with all applicable data protection laws in its provision of services, including the General Data Protection Regulation (GDPR) and maintains a Privacy Policy, which Is updated on an annual basis.

Governance

Credit Benchmark's Security, privacy, and compliance governance are overseen at the executive level with a data-driven approach to performance management, and a layered approach to risk mitigation. Intensive annual external

audits and assessments are performed on the company's security, privacy, and compliance strategy, roadmap, capabilities, policies, and performance reports by accredited agencies. Leaders and team members throughout the company maintain ongoing discussions of Credit Benchmark's strategy and roadmap with senior leadership — helping develop programs for continuous improvement. Management performs reviews of all security, privacy, and compliance performance metrics against pre-set benchmarks and goals. Each security risk is assessed according to an internal risk management framework, with significant policy changes requiring approval from Credit Benchmark's senior executive team.

Trust Center

Trust Center enables Credit Benchmark to transparently share our security posture, compliance credentials, product-level controls, and private documentation in a single, secure portal.

We empower prospective and existing clients to stay informed about our security commitments—providing up-to-date certifications, risk profiles, security bulletins, and relevant reports.

Subscribers to our Trust Center updates will be among the first to hear of new security attestations, audits, or vulnerability disclosures.

Visit our Trust Center to request access to documentation, view certifications, audits and attestations. Subscribe to receive updates directly to your mailbox. https://compliance.creditbenchmark.com/

Conclusion

Credit Benchmark recognizes the critical importance of safeguarding financial institutions' proprietary and client data. As a result, the company maintains a mature and continuously evolving security program designed to meet the expectations of highly regulated financial institutions.

Across the product, operational, and organization levels, the company has implemented leading-edge security and privacy controls. Our continued investment in security, compliance, and transparency ensures existing and prospective clients trust Credit Benchmark with sensitive credit risk insights that support strategic and regulatory decision-making.

Credit Benchmark's dedicated security team welcomes questions and concerns and strives to offer transparency to customers and potential customers alike.

Jason Rose

Chief Information Security Officer

Jason.rose@creditbenchmark.com

information.security@creditbenchmark.com

Disclaimer:

Credit Benchmark does not solicit any action based upon this report, which is not to be construed as an invitation to buy or sell any security or financial instrument. This report is not intended to provide personal investment advice and it does not take into account the investment objectives, financial situation and the particular needs of a particular person who may read this report.