CSA Consensus Assessments Initiative Questionnaire — Lite (CAIQ-Lite)

Based on CSA Cloud Controls Matrix (CCM) v4

Organisation Name	2BrightSparks Pte Ltd
Primary Contact	Michael Leaver
Contact Email	support@2brightsparks.com
Date Completed	February 20, 2026
Document Version	1.0
Review Period	Annual

Products Covered	SyncBackPro, SyncBackSE, SyncBackFree
Product Type	Desktop backup and synchronisation software
Deployment Model	On-premises (installed on customer endpoints)
Cloud Services Used	Cloud storage integration (customer-configured: FTP, SFTP, Amazon S3, Azure, Google Cloud, etc.)
Development Language	Delphi
Operating Systems Supported	Microsoft Windows
Licensing Model	Perpetual licence with optional Upgrade Assurance

Important Context	2BrightSparks develops and distributes desktop backup/synchronisation software. The software runs entirely on the customer's own infrastructure. 2BrightSparks does not host, process, or store customer data. Cloud storage connections are configured and controlled by the customer. Many cloud-specific controls in the CAIQ are therefore marked N/A, with explanations provided.

Control ID	Domain	Question	Response	Implementation Details
AIS-01	Application & Interface Security	Are secure software development lifecycle (SSDLC) practices applied for application design, development, deployment, and operation?	**Yes**	2BrightSparks follows secure development practices within the Delphi development environment, including code review, testing prior to release, and a defined change management process. Security considerations are integrated throughout the development lifecycle.
AIS-02	Application & Interface Security	Is automated application security testing performed as part of the development process?	**Partial**	Manual security testing and code review are conducted for each release. Static analysis is performed using Delphi's built-in tools. The company is working towards integrating additional automated security testing tools compatible with the Delphi ecosystem.
AIS-03	Application & Interface Security	Are application programming interfaces (APIs) designed, developed, and deployed in accordance with leading security practices?	**N/A**	SyncBack is a desktop application and does not expose public APIs or web services. Connections to cloud storage services utilise established, well-documented protocols (FTP, SFTP, S3 API, etc.) with encryption enforced.
AIS-04	Application & Interface Security	Are application security risks formally assessed and remediated?	**Yes**	Security risks are assessed during the development process. Identified vulnerabilities are prioritised and remediated prior to release. Customers can report security concerns directly to 2BrightSparks for prompt investigation and resolution.
AAC-01	Audit Assurance & Compliance	Are independent audit assurance and compliance assessments conducted at least annually?	**No**	As a small, independent software company producing desktop software, 2BrightSparks does not currently undergo independent third-party security audits (e.g. SOC 2, ISO 27001). Internal reviews of security practices and compliance requirements are conducted regularly. Third-party audits may be pursued as the business scales.
AAC-02	Audit Assurance & Compliance	Are risk-based corrective actions from audit findings tracked to closure?	**Yes**	Findings from internal reviews are tracked and addressed. Customer-reported issues and internally identified risks are logged, prioritised, and resolved through the standard development workflow.
BCR-01	Business Continuity	Is a business continuity plan established, documented, and maintained?	**Yes**	2BrightSparks maintains a Business Continuity & Disaster Recovery Plan that covers critical business operations, source code protection, website/distribution continuity, and customer support. The plan is reviewed and updated periodically.
BCR-02	Business Continuity	Are business continuity plans tested at planned intervals?	**Yes**	Business continuity procedures including backup restoration and failover processes are tested periodically to verify effectiveness. The plan is reviewed at least annually.
BCR-03	Business Continuity	Are redundant systems and backups maintained for critical business operations?	**Yes**	Source code is stored in version control with offsite backups. The company website and distribution systems have redundancy measures. Internal business data is backed up using 2BrightSparks' own SyncBack software with multiple backup destinations including offsite/cloud storage.
CCC-01	Change Control & Configuration	Are change management policies and procedures established and followed?	**Yes**	All software changes follow a defined process including development, code review, testing (unit, integration, and regression), and staged release. Changes are documented in release notes and version control history.

CCC-02	Change Control & Configuration	Is a risk assessment performed for proposed changes before deployment?	**Yes**	Changes are assessed for potential impact on security, stability, and compatibility before release. High-risk changes receive additional review and testing.
CCC-03	Change Control & Configuration	Are configuration management practices applied to ensure consistent and secure system states?	**Yes**	Build configurations are version controlled. Release builds follow a defined, repeatable process. Compiler and build environment settings are documented and maintained consistently.
CEK-01	Cryptography & Encryption	Are cryptographic controls defined and implemented to protect data?	**Yes**	SyncBack supports industry-standard encryption for data in transit (TLS/SSL for cloud connections, SFTP, FTPS) and data at rest (AES-256 encryption for backup archives). Encryption is customer-configurable based on their security requirements.
CEK-02	Cryptography & Encryption	Are encryption key management procedures established?	**Yes**	Encryption keys/passwords for backup encryption are managed by the customer. SyncBack does not transmit or store customer encryption keys externally. Password storage within profiles uses protection mechanisms. Customers are advised to maintain secure records of their encryption credentials.
CEK-03	Cryptography & Encryption	Are industry-standard cryptographic algorithms and protocols used?	**Yes**	SyncBack uses well-established cryptographic standards: AES-256 for file encryption, TLS 1.2/1.3 for secure connections, and SHA-256 or stronger for integrity verification. Deprecated or weak protocols (e.g. SSLv3, TLS 1.0) are not supported in current versions.
DCS-01	Datacenter Security	Are physical security perimeters and controls implemented to protect datacenter facilities?	**N/A**	2BrightSparks does not operate datacenters. SyncBack is desktop software that runs on the customer's own infrastructure. The company website and distribution are hosted by third-party providers with their own physical security controls.
DSP-01	Data Security & Privacy	Are data classification and handling policies established?	**Yes**	2BrightSparks classifies its own business data (source code, customer records, financial data) and applies appropriate protections. SyncBack does not access, inspect, or classify customer backup data — the software transfers and/or encrypts files as directed by the customer's configuration.
DSP-02	Data Security & Privacy	Are data privacy policies aligned with applicable regulations (e.g. GDPR, CCPA)?	**Yes**	2BrightSparks maintains a published Privacy Policy compliant with applicable regulations. Customer data collection is minimised to what is required for licence management and support. No customer backup data is collected, accessed, or processed by 2BrightSparks.
DSP-03	Data Security & Privacy	Are procedures in place for secure data disposal?	**Yes**	SyncBack provides secure file deletion capabilities for customers. 2BrightSparks follows secure disposal practices for internal business data, including secure deletion of obsolete data and proper disposal of storage media.
DSP-04	Data Security & Privacy	Are data retention policies defined and enforced?	**Yes**	2BrightSparks maintains defined retention periods for customer support records, licence data, and business records. SyncBack includes configurable backup retention/versioning features that allow customers to manage their own data retention policies.
DSP-05	Data Security & Privacy	Is personal data processed in accordance with applicable legal requirements?	**Yes**	Personal data handling is limited to customer licence and support information. Processing complies with GDPR and applicable data protection regulations. A Data Processing Addendum is available for customers who require one. SyncBack itself does not transmit personal data to 2BrightSparks.

GRC-01	Governance, Risk & Compliance	Is an information security management programme established?	**Yes**	2BrightSparks maintains an Information Security Policy that defines the company's approach to protecting information assets, managing risk, and ensuring regulatory compliance. The policy is reviewed and updated regularly.
GRC-02	Governance, Risk & Compliance	Are roles and responsibilities for information security defined and assigned?	**Yes**	Security responsibilities are defined within the company's policies. As a small company, security oversight is handled at the senior management level with direct accountability for security decisions.
GRC-03	Governance, Risk & Compliance	Is a risk management process implemented to identify, assess, and treat risks?	**Yes**	Risks are identified and assessed as part of ongoing business operations, development planning, and policy reviews. Identified risks are treated through mitigation, acceptance, or transfer as appropriate.
GRC-04	Governance, Risk & Compliance	Are applicable legal, regulatory, and contractual requirements identified and documented?	**Yes**	2BrightSparks monitors applicable regulatory requirements including GDPR, EU Cyber Resilience Act, and software licensing obligations. Compliance requirements are tracked and addressed as part of the development and business planning process.
HRS-01	Human Resources Security	Are background verification checks performed on employees and contractors?	**Partial**	As a small company, personnel are well-known to management. Appropriate due diligence is performed for any new personnel with access to sensitive systems or data.
HRS-02	Human Resources Security	Is security awareness training provided to all personnel?	**Yes**	Personnel involved in development and operations maintain current knowledge of security threats, secure coding practices, and data protection requirements relevant to their roles.
HRS-03	Human Resources Security	Are access rights revoked upon termination of employment?	**Yes**	Procedures are in place to revoke access to all systems, source code repositories, and services upon termination. Access review is part of the offboarding process.
IAM-01	Identity & Access Management	Is a formal user access management process implemented?	**Yes**	Access to development systems, source code, infrastructure, and business systems is controlled and limited to authorised personnel on a need-to-know basis.
IAM-02	Identity & Access Management	Is multi-factor authentication (MFA) enforced for access to critical systems?	**Yes**	MFA is enabled for critical systems including source code repositories, cloud hosting accounts, and administrative access to business-critical services.
IAM-03	Identity & Access Management	Are access rights reviewed on a regular basis?	**Yes**	Access rights are reviewed periodically and when personnel changes occur. The principle of least privilege is applied to system access.
IAM-04	Identity & Access Management	Are unique user identifiers assigned and shared accounts prohibited?	**Yes**	All personnel have unique credentials for system access. Shared accounts are avoided. Service accounts are used only where necessary and are appropriately secured.

IVS-01	Infrastructure & Virtualisation	Are network security controls implemented to protect the infrastructure environment?	**N/A**	2BrightSparks does not operate cloud infrastructure or host customer data. Internal development infrastructure is secured with appropriate network controls (firewalls, segmentation). Production infrastructure (website, distribution) is managed by third-party hosting providers.
IVS-02	Infrastructure & Virtualisation	Is the network architecture designed with appropriate segmentation and security zones?	**N/A**	Not applicable for a desktop software product. The company's internal network uses appropriate segmentation for development and business operations.
LOG-01	Logging & Monitoring	Are logging and monitoring capabilities implemented for critical systems and security events?	**Yes**	Logging is enabled on development systems, source code repositories, and web infrastructure. SyncBack provides comprehensive logging capabilities for customers to monitor their own backup operations, including detailed log files with configurable verbosity levels.
LOG-02	Logging & Monitoring	Are logs reviewed and retained for an adequate period?	**Yes**	System and access logs are retained for an appropriate period. Logs for critical systems are reviewed for anomalies. SyncBack provides customers with configurable log retention for their backup operations.
SEF-01	Security Incident Management	Is an incident response plan established, documented, and communicated?	**Yes**	2BrightSparks maintains an Incident Response Plan (IRP) that defines procedures for identifying, responding to, and recovering from security incidents. The plan covers roles, responsibilities, escalation procedures, communication protocols, and post-incident review.
SEF-02	Security Incident Management	Are security incidents reported and managed through a defined process?	**Yes**	Security incidents and vulnerabilities can be reported by customers via the company's support channels. Reported incidents are triaged, investigated, and addressed according to the IRP. Critical security patches are prioritised for rapid release.
SEF-03	Security Incident Management	Are post-incident reviews conducted to improve incident response?	**Yes**	Post-incident reviews are conducted following significant security events. Lessons learned are incorporated into the development process and security policies to prevent recurrence.
STA-01	Supply Chain Management	Is a software supply chain risk management process implemented?	**Yes**	2BrightSparks maintains an inventory of all third-party components and libraries used in SyncBack products. Component sources, licences, and security status are tracked. A Software Bill of Materials (SBOM) capability is being implemented in compliance with the EU Cyber Resilience Act.
STA-02	Supply Chain Management	Are third-party components assessed for security vulnerabilities?	**Yes**	Third-party components are monitored for known vulnerabilities. Binary analysis tools are used alongside manual review to identify potential security issues. Components are updated or replaced when significant vulnerabilities are discovered.
STA-03	Supply Chain Management	Are software supply chain dependencies documented and tracked?	**Yes**	A comprehensive component inventory is maintained covering all Delphi components, open-source libraries, and third-party dependencies. Licence compliance is actively managed, including identification and remediation of licence conflicts.
TVM-01	Threat & Vulnerability Management	Is a vulnerability management process established to identify and remediate vulnerabilities?	**Yes**	Vulnerabilities in SyncBack products are identified through internal testing, customer reports, and monitoring of third-party component advisories. Identified vulnerabilities are prioritised based on severity and remediated through software updates.

TVM-02	Threat & Vulnerability Management	Are vulnerability scans and/or penetration tests performed regularly?	**Partial**	Internal security testing is performed on each release. As a desktop software product, traditional network penetration testing is less applicable. Binary analysis and code review are used to identify vulnerabilities. External penetration testing of web infrastructure may be pursued as the compliance programme matures.
TVM-03	Threat & Vulnerability Management	Are security patches applied in a timely manner?	**Yes**	Security patches for SyncBack are prioritised and released promptly when vulnerabilities are identified. Customers on Upgrade Assurance receive updates automatically. Third-party component updates are monitored and applied as part of the regular release cycle.
UEM-01	Endpoint Management	Are endpoint security controls implemented on devices used for development and operations?	**Yes**	Development and business systems are protected with endpoint security software, operating system updates, and secure configuration. Access to development environments is restricted to authorised devices.

CAIQ-Lite Response Summary

Domain	Yes	Partial	No	N/A	Total
Application & Interface Security	2	1	0	1	4
Audit Assurance & Compliance	1	0	1	0	2
Business Continuity	3	0	0	0	3
Change Control & Configuration	3	0	0	0	3
Cryptography & Encryption	3	0	0	0	3
Datacenter Security	0	0	0	1	1
Data Security & Privacy	5	0	0	0	5
Governance, Risk & Compliance	4	0	0	0	4
Human Resources Security	2	1	0	0	3
Identity & Access Management	4	0	0	0	4
Infrastructure & Virtualisation	0	0	0	2	2
Logging & Monitoring	2	0	0	0	2
Security Incident Management	3	0	0	0	3
Supply Chain Management	3	0	0	0	3
Threat & Vulnerability Management	2	1	0	0	3
Endpoint Management	1	0	0	0	1

TOTALS	**38**	**3**	**1**	**4**	**46**

Compliance Rate (Yes + Partial / Applicable) 97.6%

Notes

- N/A responses reflect that SyncBack is desktop software — 2BrightSparks does not operate cloud infrastructure or host customer data.
- 'Partial' responses indicate controls that are in place but where formalisation or additional tooling is being pursued.
- 2BrightSparks is actively working towards EU Cyber Resilience Act compliance (deadline: 2027), including SBOM implementation.
- This questionnaire should be reviewed and updated annually or when significant changes occur.
- Items marked [Contact Name] and [Contact Email] on the Cover sheet should be completed before distribution.