

Brightwater Metrics (sample)

Information security record: decisions and approvals, not a certificate or an audit opinion.

Package code	340E-8865-E3ED
Period	Recorded 8 Sep to 16 Oct 2026. It shows design and approval, not operation over time.
Prepared for	Not named; the company says who it is for when it sends the package
Prepared by	Brightwater Metrics (sample), from its Kanonik workspace
Records	66, one PDF each in the Records folder; index on page 14.
Seal	Sealed in Kanonik, 19 Oct 2026, 12:00 UTC. Anyone can confirm nothing changed (page 17).

Where each framework stands

Applicable is what the company states applies to it; section 4 says how many of those it states as implemented. A note is an open finding on the row's control or a record the row needs; gaps of a whole framework are under Not held as records.

Framework	Applicable	Rows with a note	Page
SOC 2	16 of 18 criteria	1	6
NIST CSF	15 of 16 subcategories	1	8

Open points

Audit findings	2 SOC 2 nonconformities, 1 still open; 2 controls found operating effectively (page 4).
Approved by their author	15 of 150 record versions were approved by Priya Venkataram, who drafted them (page 11).
Not fully approved	policy BM-POL-01 , one approver where two were needed; policy BM-POL-02 , one approver where two were needed (page 5).
Risk acceptance	Risk BM-RSK-05 has the acceptance BM-RA-01 (page 10).

Sending this on? Send the downloaded file,
Brightwater Metrics (sample) audit package 340E-8865-E3ED.tar.gz, not this PDF.

Contents

1. Scope and what is not in this package	3
2. Findings and corrective action	4
3. Exceptions, accepted risks and items not fully approved	5
4. Statements of Applicability	6
4.1 SOC 2 (AICPA Trust Services Criteria, 2017 / rev. 2022)	6
4.2 NIST Cybersecurity Framework (CSF) 2.0	8
5. Risk register	10
6. Approvals and who could approve	11
7. How to sample	13
8. Record index	14
9. The seal check	17

The folders

Records	One PDF per record, named by its reference and title, in a folder per kind. 66 records.
Tables	Applicability per framework (one spreadsheet each), Links between records.csv, Approvals.csv and Record population.csv.
Verification	The seal check (section 9).

Words used

Seal	A fingerprint of every record and approval, taken when the package was made. The check confirms nothing changed since.
Statement of Applicability	For each requirement of a framework: whether it applies, why, and which controls meet it.
Basis	Why a requirement applies: the law, a contract, or the risks its controls treat.
Stated	What Brightwater Metrics (sample) says and approved, not an auditor's conclusion.
Log entry, entry hash	The number of the record's entry in the sealed log (Verification/events.jsonl) and that entry's fingerprint.
Automatic check	Kanonik's rule check of each version before approval; it passes it or asks a person to review.
Record version	Each time a record or a table row is approved and sealed is one version: 150 in this package, 63 for the 62 records listed by kind and 87 for rows kept in Tables. The Records folder holds 66 records in all: those 62 plus 4 more that are not listed by kind in the index. A record page with more than one shows them as Sealed versions.
Document version	The number the document gives itself, such as 2.1 on a policy. It is not a count of seals.
Requirement mapping	A link from a control to a framework requirement it meets; shown as Met by.
References	BM-POL policy, BM-PRC procedure, BM-CTL control, BM-RSK risk, BM-TST control test, BM-EV evidence, BM-AF audit finding, BM-REM corrective action, BM-EXC exception, BM-RA risk acceptance, BM-AST asset, BM-VND vendor, BM-OBL obligation, BM-AUD audit session.

1. Scope and what is not in this package

Who asks for proof

Asked by	What they require
Tamarind Row Restaurants (sample customer) Contract	Tamarind Row's agreement, signed in August 2026, requires Brightwater to deliver a SOC 2 report by 31 March 2027. Source: Master agreement, section 14.2 (security assurance); deadline 2027-03-31
EU supervisory authorities Regulation	Brightwater holds names and work email addresses of customers' restaurant staff in the EU, so it is a processor under the GDPR. Source: Data processing terms in the customer agreement

Frameworks

Framework	Decision	Reason or limit recorded	Decided	Log entry
SOC 2	Chosen	The report covers the Brightwater Analytics platform and the processes that run it. It does not cover customers' own systems, or the cloud provider's data centres.	Priya Venkataram, 9 Sep 2026	43
NIST CSF	Applies		Priya Venkataram, 9 Sep 2026	45
GDPR	Applies		Priya Venkataram, 9 Sep 2026	44

The date is the decision date Brightwater Metrics (sample) gave; every decision was recorded in the log inside the period (entry numbers).

Not in this package

The evidence files themselves. Each evidence record names where the file is kept and its SHA-256; ask Brightwater Metrics (sample) for the files you sample.

2 entries left out as commercially confidential (prices and invoices); the seal check still covers them.

Records of operation over time (tickets, change records, access logs): this package records design and approval. Draw those populations from Brightwater Metrics (sample)'s own systems.

2. Findings and corrective action

Marguerite Oyelaran raised 2 findings with an exception; later lists close 1 of them, 1 stay open.

Ref	Finding	Grade	Control
BM-AF-01	NC-1: 3 of 40 sampled critical findings were fixed after the seven-day limit (9, 11 and 14 days), and the weekly overdue report was missing in 2 of 13 weeks.	Minor	BM-CTL-06 Finding and fixing known weaknesses
BM-AF-02	NC-2: no restore test was run in the third quarter, so the quarterly check did not operate. Nightly backups were running.	Minor	BM-CTL-07 Backups and restore tests

1 corrective action is recorded: [BM-REM-01](#). For the other findings none is recorded. No due date and no root cause are recorded for any finding.

Operating effectively (2)

Ref	Control	What the auditor inspected	Audit, round
BM-AF-03	BM-CTL-02 Quarterly review of who has access	OK-1: the Q3 access review covered all four systems, every decision is recorded and removals closed within five working days.	SOC 2, round 1
BM-AF-04	BM-CTL-07 Backups and restore tests	OK-2: follow-up to NC-2. A restore of the latest backup was observed on 13 October: 41 minutes, row counts matched on all 18 tables. NC-2 is closed.	SOC 2, round 2

3. Exceptions, accepted risks and items not fully approved

Not fully approved, or incompletely recorded

Ref	Item	What the record shows
BM-POL-01	The policy Information Security Policy	Policy on 11 Sep 2026, 14:22 UTC by Priya Venkataram: one approver where two were needed
BM-POL-02	The policy Access Control Policy	Policy on 11 Sep 2026, 14:22 UTC by Priya Venkataram: one approver where two were needed

Exception **BM-EXC-01**

Until 14 September 2026 Priya Venkataram was the only person who could approve in this workspace. She approved the Information Security Policy and the Access Control Policy on 11 September although she wrote them. A second approver, Tomas Achebe, joined on 14 September. Until he has read both policies they rest on one person's approval.

Approved	16 Sep 2026, 11:00 UTC; Tomas Achebe
Compensating control	BM-CTL-13 Second look at security policy changes
Expires	15 Dec 2026, reviewed every 30 days
Plan	From 14 September every security policy is approved by someone other than its author. Tomas reads the two policies approved on 11 September by 30 September and records the read under BM-CTL-13 , which closes this exception.

Risk acceptance **BM-RA-01**

Use of unapproved tools is limited by the approved tools list and the monthly expense review. What remains is low-value, non-customer information in a few team tools, which the VP Engineering accepts and will look at again in April 2027.

Risk	BM-RSK-05 Staff use unapproved tools
Residual	Likelihood possible, impact minor
Accepted	Tomas Achebe, 15 Oct 2026, 09:30 UTC

4. Statements of Applicability

One table per framework (basis and stated: see page 2). Met by gives the control references; each opens the control. Note shows only what differs, such as an open audit finding against the row's control or a record the row needs that is not recorded.

4.1 SOC 2 (AICPA Trust Services Criteria, 2017 / rev. 2022)

16 of 18 apply, 15 stated as implemented. Proposed by Priya Venkataram; approved by Tomas Achebe, 21 Sep 2026.

Not applicable, with the reason recorded

CC6.4 Physical access to facilities. Not applicable: the company is fully remote and has no offices or data centres. Physical protection of servers sits with the cloud provider, whose own report we review each year.

P6.6 Notifying people of breaches. Not applicable to this report: the company acts as a processor and customers notify their own users; breach notice to customers is covered under incident response.

Criteria that apply (16)

Ref	Criterion	Basis	Met by	Evidence	Note
A1.2	Safeguards against outages and loss	BM-RSK-03, BM-RSK-04	BM-CTL-07	BM-EV-008	
A1.3	Proving recovery works	BM-RSK-03, BM-RSK-04	BM-CTL-07	BM-EV-008	
CC1.2	Independent oversight	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-01		
CC1.3	Clear roles and reporting lines	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-01		
CC1.4	Hiring and keeping skilled people	BM-RSK-01	BM-CTL-10	BM-EV-005	
CC5.3	Controls written into policy and practice	BM-RSK-05	BM-CTL-13		
CC6.1	Protecting systems and data from unauthorised access	BM-RSK-01	BM-CTL-04	BM-EV-002	
CC6.2	Granting and removing user accounts	BM-RSK-01	BM-CTL-02, BM-CTL-03	BM-EV-001	
CC6.3	Access matches the job	BM-RSK-01	BM-CTL-02	BM-EV-001	
CC6.7	Controlling how data moves	BM-RSK-03	BM-CTL-11		
CC7.1	Spotting weak points and configuration drift	BM-RSK-02	BM-CTL-06	BM-EV-004	1 open

Ref	Criterion	Basis	Met by	Evidence	Note
CC7.2	Monitoring for suspicious activity	BM-RSK-02	BM-CTL-12		
CC7.3	Deciding whether an event is an incident	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-08	BM-EV-006	
CC7.4	Responding to incidents	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-08	BM-EV-006	
CC8.1	Controlled changes to systems	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-05	BM-EV-003	
CC9.2	Managing vendors and partners	BM-RSK-04	BM-CTL-09	BM-EV-007	

4.2 NIST Cybersecurity Framework (CSF) 2.0

15 of 16 apply, 14 stated as implemented. Proposed by Priya Venkataram; approved by Tomas Achebe, 21 Sep 2026.

Not applicable, with the reason recorded

PR.IR-01 Networks and environments are protected from unauthorized logical access and usage. Not applicable as a separate step: the company has no physical network of its own; networks are managed by the cloud provider and covered under supplier review.

Subcategories that apply (15)

Ref	Subcategory	Basis	Met by	Evidence	Note
DE.CM-01	Networks and network services are monitored to find potentially adverse events	BM-RSK-02	BM-CTL-12		
GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-01		
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	BM-RSK-05	BM-CTL-13		
GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-01		
GV.SC-04	Suppliers are known and prioritized by criticality	BM-RSK-04	BM-CTL-09	BM-EV-007	
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	BM-RSK-02	BM-CTL-06	BM-EV-004	1 open
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-03		
PR.AA-03	Users, services, and hardware are authenticated	BM-RSK-01	BM-CTL-04	BM-EV-002	

Ref	Subcategory	Basis	Met by	Evidence	Note
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	BM-RSK-01	BM-CTL-02	BM-EV-001	
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	BM-RSK-01	BM-CTL-10	BM-EV-005	
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	BM-RSK-03	BM-CTL-11		
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	BM-RSK-03	BM-CTL-11		
PR.DS-11	Backups of data are created, protected, maintained, and tested	BM-RSK-03 , BM-RSK-04	BM-CTL-07	BM-EV-008	
PR.PS-01	Configuration management practices are established and applied	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-05	BM-EV-003	
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	Contract, Tamarind Row Restaurants (sample customer)	BM-CTL-08	BM-EV-006	

5. Risk register

5 risks, owned by Priya Venkataram and Tomas Achebe, scored before treatment on the recorded scale (likelihood: unlikely, possible, likely; impact: minor, major, severe). The risks carry no residual rating or acceptance criteria of their own; a residual rating appears only on an accepted risk, in section 3.

Ref	Risk	Likelihood	Impact	Treatment	Treated by
BM-RSK-01	An attacker phishes or guesses a staff password and signs in to the identity provider or production, reading customer sales data.	Possible	Major	Mitigate	BM-CTL-02 BM-CTL-04 BM-CTL-10
BM-RSK-02	Ransomware reaches a laptop or a server through an unpatched weakness and spreads to production, stopping the service.	Possible	Severe	Mitigate	BM-CTL-06 BM-CTL-12
BM-RSK-03	After data loss or corruption the latest backup turns out to be incomplete or too slow to restore, and customers lose data or wait days.	Unlikely	Severe	Mitigate	BM-CTL-07 BM-CTL-11
BM-RSK-04	A regional outage at the cloud provider takes the platform offline for more than four hours.	Unlikely	Major	Mitigate	BM-CTL-07 BM-CTL-09
BM-RSK-05	Staff sign up for unapproved online tools and paste company information into them, outside our controls.	Likely	Minor	Accept; acceptance BM-RA-01	BM-CTL-13

6. Approvals and who could approve

15 of 150 versions were approved by Priya Venkataram, who drafted them; the two gaps are in section 3. The automatic check asked for review on 0: 0 then had a second person, 0 one person (0 their author).

Record kind	Versions	Second person	Author (routine)	One person, no reason	Second person missing	Not recorded	Check asked for review
Policies	4	2				2	
Procedures	2	2					
Controls	14	14					
Risks	5	5					
Control tests	12	12					
Evidence	8	8					
Audit findings	4	4					
Corrective actions	1	1					
Exceptions	1	1					
Risk acceptances	1	1					
Assets	5		5				
Vendors	3		3				
Obligations	2		2				
Audit sessions	1	1					
Kept in Tables only							
Applicability decisions	34	34					
Requirement mappings	32	32					
Links between records	18	18					
Framework choices	1		1				
Framework applicability	2		2				
Total	150	135	13			2	

Policies, procedures, controls, applicability decisions, exceptions and risk acceptances need a second person when one exists; a corrective action may be approved by its author. Of 20 evidence and control-test versions, 0 were sealed by their author as routine records; the rest were approved as the table shows. The automatic check rejected none of the approved items. Approvals.csv lists every approval with its records.

Approvals by person

Person	Record versions approved	Of these, their own drafts
Tomas Achebe	92	0
Priya Venkataram	58	15
Marguerite Oyelaran	0	0
Nora Lindqvist	0	0

Who could approve

Person	Can	From
Priya Venkataram	Propose and approve; administrator	8 Sep 2026, 09:04 UTC
Nora Lindqvist	Read only	8 Sep 2026, 09:05 UTC
Tomas Achebe	Approve as reviewer	14 Sep 2026, 09:01 UTC
Marguerite Oyelaran	Read only	5 Oct 2026, 08:01 UTC

7. How to sample

Tables/Record population.csv has one row per sealed record version: when it was proposed, approved and sealed, by whom, how, and what the automatic check said. A record with several versions has one row per version.

Population	Records	Versions	Where
Policies	4	4	Records/Policies
Procedures	2	2	Records/Procedures
Controls	13	14	Records/Controls
Risks	5	5	Records/Risks
Control tests	12	12	Records/Control tests
Evidence	8	8	Records/Evidence
Audit findings	4	4	Records/Audit findings
Corrective actions	1	1	Records/Corrective actions
Exceptions	1	1	Records/Exceptions
Risk acceptances	1	1	Records/Risk acceptances
Assets	5	5	Records/Assets
Vendors	3	3	Records/Vendors
Obligations	2	2	Records/Obligations
Audit sessions	1	1	Records/Audit sessions
Listed by kind	62	63	
Also with a PDF	4		Records/; not listed by kind above
All records	66		Records/
Kept in Tables only			
Applicability decisions		34	Tables/Applicability (one per framework), Applies and Basis
Requirement mappings		32	Tables/Applicability (one per framework), Met by and Why
Links between records		18	Tables/Links between records.csv
Framework choices		1	Section 1, Frameworks, by log entry
Framework applicability		2	Section 1, Frameworks, by log entry
Table rows		87	
All sealed versions		150	

Tracing one sample

1. Pick a reference in the population, for example BM-CTL-01.
2. Open Records/Controls/BM-CTL-01 Security leadership and oversight.pdf. It lists the requirements it meets, its evidence, tests and findings, and its log entry number.
3. The seal check (section 9) confirms every log entry at once; to see one, find its number in Verification/events.jsonl.

8. Record index

Every record in Records, with its reference. Kanonik gives a reference to records that had none (risks, evidence, tests and findings). Each reference opens the record when the package is unpacked.

Ref	Title	Document version
Policies (4)		
BM-POL-01	Information Security Policy	1.0
BM-POL-02	Access Control Policy	1.0
BM-POL-03	Incident Response Policy	1.0
BM-POL-04	Acceptable Use Policy	1.0
Procedures (2)		
BM-PRC-01	Joiner, mover and leaver procedure	1.0
BM-PRC-02	Backup and restore procedure	1.0
Controls (13)		
BM-CTL-01	Security leadership and oversight	
BM-CTL-02	Quarterly review of who has access	
BM-CTL-03	Starting, changing and leaving staff	
BM-CTL-04	Two-step sign-in for staff	
BM-CTL-05	Reviewed and approved changes	
BM-CTL-06	Finding and fixing known weaknesses	
BM-CTL-07	Backups and restore tests	
BM-CTL-08	Responding to security incidents	
BM-CTL-09	Checking suppliers before and during use	
BM-CTL-10	Security training for everyone	
BM-CTL-11	Encrypting customer data	
BM-CTL-12	Logging and alerts on production	
BM-CTL-13	Second look at security policy changes	
Risks (5)		
BM-RSK-01	A staff account is taken over	
BM-RSK-02	Ransomware on a laptop or server	
BM-RSK-03	A backup cannot be restored	
BM-RSK-04	The cloud provider has a long outage	
BM-RSK-05	Staff use unapproved tools	
Control tests (12)		
BM-TST-01	Design test of security leadership and oversight	

Ref	Title	Document version
BM-TST-02	Operating test of quarterly review of who has access	
BM-TST-03	Operating test of starting, changing and leaving staff	
BM-TST-04	Operating test of two-step sign-in for staff	
BM-TST-05	Operating test of reviewed and approved changes	
BM-TST-06	Operating test of finding and fixing known weaknesses	
BM-TST-07	Operating test of backups and restore tests	
BM-TST-08	Design test of responding to security incidents	
BM-TST-09	Operating test of checking suppliers before and during use	
BM-TST-10	Operating test of security training for everyone	
BM-TST-11	Operating test of second look at security policy changes	
BM-TST-12	Operating test of backups and restore tests (re-test)	
Evidence (8)		
BM-EV-001	Q3 2026 access review sheet	
BM-EV-002	Two-step sign-in settings export	
BM-EV-003	Production change sample, Aug to Sep 2026	
BM-EV-004	Weekly vulnerability scan, 28 Sep 2026	
BM-EV-005	Security training completion report, 2026	
BM-EV-006	Incident rehearsal notes, 2 Sep 2026	
BM-EV-007	Supplier review: Stratus Row Hosting	
BM-EV-008	Restore test report, 12 Oct 2026	
Audit findings (4)		
BM-AF-01	Audit finding: deficient on BM-CTL-06 Finding and fixing known weaknesses	
BM-AF-02	Audit finding: deficient on BM-CTL-07 Backups and restore tests	
BM-AF-03	Audit finding: operating effectively on BM-CTL-02 Quarterly review of who has access	
BM-AF-04	Audit finding: operating effectively on BM-CTL-07 Backups and restore tests	
Corrective actions (1)		
BM-REM-01	Restore test after the backup finding	
Exceptions (1)		
BM-EXC-01	Sole approver for the first two security policies	
Risk acceptances (1)		
BM-RA-01	Accept the unapproved-tools risk until April 2027	
Assets (5)		

Ref	Title	Document version
BM-AST-01	Brightwater Analytics platform (production)	
BM-AST-02	Customer data warehouse	
BM-AST-03	Company identity provider	
BM-AST-04	Staff laptops	
BM-AST-05	Build and release pipeline	
Vendors (3)		
BM-VND-01	Stratus Row Hosting (sample supplier)	
BM-VND-02	Plumb Line Workspace (sample supplier)	
BM-VND-03	Linehaul Support Desk (sample supplier)	
Obligations (2)		
BM-OBL-01	Tamarind Row Restaurants: SOC 2 report by March 2027	
BM-OBL-02	GDPR processor duties for EU customer data	
Audit sessions (1)		
BM-AUD-01	Audit session: 5 Oct 2026 to 15 Dec 2026	

9. The seal check

No Kanonik account or internet connection is needed.

1. Open Verification/verify.html in a browser and drop the package file onto it, or choose it: Brightwater Metrics (sample) audit package 340E-8865-E3ED.tar.gz. Nothing leaves your computer. Or, from a command line inside the unpacked folder, run `python3 Verification/chain/verify.py`.
2. Read the result: Passed, Passed with notes (nothing changed; a note says what could not be fully confirmed), or Failed (the result names the check).
3. Check that it shows the package code 340E-8865-E3ED.

What the check reports for this package

All 401 log entries are unchanged and in order (the 150 record versions, plus approvals, automatic check results, drafting rounds, AI instruction sets loaded and AI tool calls, which carry no record), every approval followed the approval rules except BM-POL-01 (one approver where two were needed) and BM-POL-02 (one approver where two were needed), section 3, and every file in the package matches the list of file hashes that Kanonik signed with the same key (Verification/package_seal.json). The seal is from Kanonik's public sample key: synthetic data, not a customer record.

Seal details for your working papers

Last log entry hash	340e8865e3ed20bcdfb404453dae3d6e772069d97f2f55761728d183c62417a8
Package code	340E-8865-E3ED: the first 12 characters of that hash
Entries	401, the last sealed 19 Oct 2026, 12:00 UTC
Signing key	kanonik-public-sample-2026-10-04, ECDSA P-384; SHA-256 of the public key bd2689adf99a28d57e1a0174a3bc835b772ef02b437a5a59f9fd3bbd19fe277f
Where the key is trusted from	The checker compares the signature with Kanonik's pinned key list. The copy in this package travels with it, so check the key independently: Kanonik publishes its keys at https://kanonik.ai/well-known/kanonik-chain-root-keys.json , and <code>python3 Verification/chain/verify.py --online</code> compares against that list.

The seal shows that the record did not change after sealing and who approved each item, not that a requirement is met.