traztech

Cybersecurity & Compliance Consulting

Phase 1 Gap Analysis Report

Specimen document

Kestrel Data Systems Inc.

Prepared for	Kestrel Data Systems Inc.
Prepared by	Jacob Masse, Principal, TrazTech Inc.
Date	September 10, 2026
Reference	SAMPLE-GAP-01

Specimen document

This is a published example of the report TrazTech delivers, not a record of any engagement. The client, the systems, the control answers and the dates below are invented for illustration. Nothing here describes a real organisation.

Contents

1. Engagement Scope and Decisions

This document is the Phase 1 deliverable under the TrazTech audit-readiness engagement. Phase 1 is a comprehensive gap analysis and review of Kestrel Data Systems Inc.'s current position against the SOC 2 control set. Remediation, policy formalisation and audit firm coordination are Phase 2 scope under a separate statement of work.

The following decisions were captured at kickoff and hold across the engagement.

Decision	Position
Which Trust Services Categories are in scope?	Security (Common Criteria) - required, Availability, Confidentiality, Privacy
Do you have physical sites in scope?	Fully remote, no office holding in-scope data
Type I or Type II?	Type I (point in time)
Criteria in scope	56 assessed individually against the SOC 2 control set

Decision	Position
Engagement delivery	Conducted remotely. All evidence submitted and reviewed through the TrazTech compliance portal, which is the record of the engagement rather than a copy of it.
Deliverable status	Assessment and framing. This report does not remediate, and no position stated here should be read as an audit opinion.

2. Assessment Methodology

Engagement overview

This report presents the findings of a SOC 2 readiness assessment conducted by TrazTech Inc. for Kestrel Data Systems Inc. The assessment evaluates the design and implementation status of controls against the applicable criteria as at the report date.

Observations are based on documentation review, configuration evidence submitted to the portal, and the systems the workspace records. Where documentation is insufficient to confirm a control, the position is recorded as Partial or Gap identified rather than assumed in the client's favour. An unanswered criterion counts against the readiness figure, because "we do not know" is not a neutral position in front of an auditor.

State definitions

State	Meaning for Phase 1
Met	Evidence provided in Phase 1 is sufficient to satisfy audit expectations for this criterion.
Partial	Substantive material is in place; a specific delta remains and is documented and cross-referenced to a findings register entry.
Gap identified	The control has been actively assessed in Phase 1 and confirmed not to currently exist. Carried into Phase 2 remediation scope.
Not assessed	The criterion was not answered and no evidence was submitted against it. Treated as a gap for scoring, and resolved by answering it.

3. Basis of Assessment and Coverage

Phase 1 is a confirmation and framing exercise, not a remediation exercise. The report treats the full in-scope control universe, 56 criteria, as the denominator, because that is the denominator the auditor will use. Assessing against a reduced set would produce a more flattering figure and a less useful one.

Positions stated in this report reflect the evidence available at the report date. A control recorded as Partial is not a criticism of intent; it is a statement that the artifact an auditor would sample does not yet exist in the form they would accept.

4. Executive Summary

Assessment of 56 criteria across 12 control families. Detailed per-criterion findings follow in section 6.

18	23	12	3	56
Met	Partial	Gap identified	Not assessed	Total

Overall readiness stands at **53 percent**. 38 criteria require work before an auditor would accept them, of which 3 are rated critical and 12 high. The findings register at section 7 carries each one with a severity and a cross-reference to the criteria it affects.

Position by category

Category	Total	Met	Partial	Gap	Not assessed
CC1 - Control Environment	5	2	2	1	0
CC2 - Communication and Information	3	1	1	1	0
CC3 - Risk Assessment	4	0	2	1	1
CC4 - Monitoring Activities	2	0	1	1	0
CC5 - Control Activities	3	1	2	0	0
CC6 - Logical and Physical Access Controls	8	5	2	1	0
CC7 - System Operations	5	2	2	1	0
CC8 - Change Management	1	1	0	0	0
CC9 - Risk Mitigation	2	0	1	1	0
A1 - Availability	3	2	1	0	0
C1 - Confidentiality	2	1	1	0	0
P - Privacy	18	3	8	5	2

Summary

Metric	Count
Total criteria assessed	56
Met	18
Partial	23
Gap identified	12
Not assessed	3
Critical severity findings	3
High severity findings	12
Evidence artifacts collected	78 of 128

5. Readiness by Control Family

A single readiness figure conceals the shape of the problem: a strong overall position can rest on one family at zero. Broken out below, the families needing runway are visible at a glance, as are those where evidence collection can begin immediately.

Family	In scope	Position	Ready
CC1 - Control Environment	5		60%
CC2 - Communication and Information	3		50%
CC3 - Risk Assessment	4		25%
CC4 - Monitoring Activities	2		25%
CC5 - Control Activities	3		67%
CC6 - Logical and Physical Access Controls	8		75%
CC7 - System Operations	5		60%
CC8 - Change Management	1		100%

Family	In scope	Position	Ready
CC9 - Risk Mitigation	2		25%
A1 - Availability	3		83%
C1 - Confidentiality	2		75%
P - Privacy	18		39%

met partial gap identified not assessed

6. Full Per-Criterion Assessment

Each of the 56 criteria in scope is assessed below. The State column reflects the position at report date. The Note column summarises the current observation. The G/R column cross-references the findings register entry where one applies.

CC1 - Control Environment

Criterion	Title	State	Note	G/R
CC1.1	Commitment to integrity and ethical values	Met	Evidence submitted and accepted for this criterion.	
CC1.2	Board or equivalent exercises oversight	Partial	The auditor is checking that security is not self-graded by the only person who would look bad if it were failing.	G-25
CC1.3	Structures, reporting lines, and authority are defined	Met	Evidence submitted and accepted for this criterion.	
CC1.4	Attracts, develops, and retains competent people	Gap identified	Most breaches at this company size start with a person, so the auditor checks whether you hire and train deliberately.	G-07
CC1.5	Holds people accountable for control responsibilities	Partial	The auditor is testing whether the control owner has any real incentive to run the control on time.	G-35

CC2 - Communication and Information

Criterion	Title	State	Note	G/R
CC2.1	Uses relevant, quality information	Gap identified	Controls that run off stale or hand-typed data fail the moment an auditor samples against the source system.	G-05
CC2.2	Communicates internally	Partial	A policy nobody has read is not a control, and the auditor will ask a random employee how they would report a phishing email.	G-19
CC2.3	Communicates externally	Met	Evidence submitted and accepted for this criterion.	

CC3 - Risk Assessment

Criterion	Title	State	Note	G/R
CC3.1	Specifies objectives clearly enough to assess risk	Partial	Without a written boundary and objective, any risk register is arbitrary and the auditor cannot judge whether you missed something.	G-34
CC3.2	Identifies and analyses risk	Gap identified	The auditor wants to see that your controls were chosen because of identified risk, not copied from a template.	G-11
CC3.3	Considers the potential for fraud	Not assessed	Fraud risk is called out separately in the criteria, so a register with no insider scenarios reads as incomplete.	G-14
CC3.4	Identifies and assesses significant change	Partial	Most control failures at growing companies happen right after a change nobody assessed.	G-18

CC4 - Monitoring Activities

Criterion	Title	State	Note	G/R
CC4.1	Performs ongoing and separate evaluations	Gap identified	A control that nobody tests is a control that has probably been broken for months.	G-12
CC4.2	Evaluates and communicates deficiencies	Partial	The auditor is testing the loop, not the finding: a deficiency you found and closed looks better than one you never had.	G-33

CC5 - Control Activities

Criterion	Title	State	Note	G/R
CC5.1	Selects and develops control activities	Partial	The auditor wants to see design intent, that you chose these controls to address specific identified risks.	G-32
CC5.2	Selects and develops technology general controls	Met	Evidence submitted and accepted for this criterion.	
CC5.3	Deploys control activities through policy and procedure	Partial	The auditor tests whether the documented process is the one people actually followed during the period.	G-31

CC6 - Logical and Physical Access Controls

Criterion	Title	State	Note	G/R
CC6.1	Restricts logical access to protect information assets	Met	Evidence submitted and accepted for this criterion.	
CC6.2	Registers and authorises new users before granting access	Met	Evidence submitted and accepted for this criterion.	
CC6.3	Manages access based on roles and least privilege	Partial	Least privilege is what limits blast radius when one account is eventually compromised.	G-30
CC6.4	Restricts physical access to facilities and hardware	Met	Evidence submitted and accepted for this criterion.	
CC6.5	Disposes of data and hardware securely	Gap identified	Recovered data from a disposed laptop or an unattached storage volume is a breach with no attacker required.	G-01
CC6.6	Protects against threats from outside the system boundary	Met	Evidence submitted and accepted for this criterion.	
CC6.7	Restricts movement of information to authorised users	Partial	The auditor is checking that data in motion is protected and that bulk movement is deliberate and logged.	G-29
CC6.8	Prevents and detects unauthorised software	Met	Evidence submitted and accepted for this criterion.	

CC7 - System Operations

Criterion	Title	State	Note	G/R
CC7.1	Detects configuration changes and new vulnerabilities	Met	Evidence submitted and accepted for this criterion.	
CC7.2	Monitors system components for anomalies	Partial	The auditor wants proof that alerts were triaged during the period, not just that a monitoring tool was purchased.	G-38
CC7.3	Evaluates security events and decides on incidents	Gap identified	The auditor tests whether a consistent, documented judgement was applied rather than case-by-case improvisation.	G-08
CC7.4	Responds to identified security incidents	Met	Evidence submitted and accepted for this criterion.	
CC7.5	Recovers from identified security incidents	Partial	The auditor is checking that you can return to normal operation on a known timeline rather than hoping.	G-28

CC8 - Change Management

Criterion	Title	State	Note	G/R
CC8.1	Authorises, designs, tests, and approves changes	Met	Evidence submitted and accepted for this criterion.	

CC9 - Risk Mitigation

Criterion	Title	State	Note	G/R
CC9.1	Mitigates risk from business disruption	Partial	The auditor wants to see deliberate choices about disruption, including what you decided to accept.	G-36
CC9.2	Assesses and manages vendor and partner risk	Gap identified	Your customers hold you responsible for your subprocessors, and so does the auditor.	G-10

A1 - Availability

Criterion	Title	State	Note	G/R
A1.1	Manages capacity to meet availability commitments	Met	Evidence submitted and accepted for this criterion.	
A1.2	Maintains backup, recovery, and environmental protections	Partial	Backups you never verified are the difference between a bad day and losing the company.	G-27
A1.3	Tests recovery procedures	Met	Evidence submitted and accepted for this criterion.	

C1 - Confidentiality

Criterion	Title	State	Note	G/R
C1.1	Identifies and protects confidential information	Met	Evidence submitted and accepted for this criterion.	
C1.2	Disposes of confidential information when no longer needed	Partial	A deletion promise you cannot demonstrate is a contractual claim your auditor will not sign off on.	G-26

P - Privacy

Criterion	Title	State	Note	G/R
P1.1	Provides notice about privacy practices	Gap identified	Every privacy criterion after this one is measured against what your notice said you would do.	G-03
P2.1	Obtains and documents consent and choice	Partial	A consent flag with no timestamp or notice version cannot be defended to an auditor or a regulator.	G-37
P3.1	Collects personal information consistently with objectives	Not assessed	Data minimisation is the cheapest privacy control you have, because data you never collected cannot leak.	G-15
P3.2	Obtains explicit consent for sensitive personal information	Gap identified	Sensitive data attracts higher penalties and higher scrutiny, so the consent bar is deliberately higher.	G-06

Criterion	Title	State	Note	G/R
P4.1	Limits use of personal information to stated purposes	**Partial**	Purpose creep is the most common privacy finding, and it usually happens without anyone deciding to do it.	G-24
P4.2	Retains personal information only as long as needed	**Met**	Evidence submitted and accepted for this criterion.	
P4.3	Disposes of personal information securely	**Partial**	A deletion request you cannot evidence to completion is a promise you did not keep.	G-22
P5.1	Grants data subjects access to their personal information	**Gap identified**	The auditor samples real requests and measures your response time against the commitment in your notice.	G-04
P5.2	Corrects, amends, or appends personal information on request	**Partial**	Correction rights are only meaningful if the fix reaches every copy you created.	G-21
P6.1	Discloses personal information only with consent or authority	**Met**	Evidence submitted and accepted for this criterion.	
P6.2	Keeps a record of authorised disclosures	**Not assessed**	You cannot honour an accounting-of-disclosures request without a record you kept at the time.	G-13
P6.3	Keeps a record of unauthorised disclosures	**Partial**	The auditor looks for a maintained log, because a period with zero recorded privacy incidents usually means nobody was recording them.	G-20
P6.4	Obtains privacy commitments from third parties	**Gap identified**	Your obligations follow the data, so a vendor with no privacy commitment is an unbounded liability.	G-09
P6.5	Obtains commitment from third parties to report unauthorised disclosure	**Partial**	You are on the hook for your subprocessor breach, and your clock starts when they tell you.	G-17
P6.6	Notifies affected parties of unauthorised disclosure	**Met**	Evidence submitted and accepted for this criterion.	

Criterion	Title	State	Note	G/R
P6.7	Provides an accounting of personal information held and disclosed	**Partial**	This is the criterion that proves your disclosure records are usable, not just stored.	G-23
P7.1	Maintains accurate and complete personal information	**Gap identified**	Decisions made from inaccurate personal data cause real harm, which is exactly what this criterion is about.	G-02
P8.1	Handles privacy complaints and disputes	**Partial**	Regulators and auditors both look at complaint handling as the clearest signal of whether the privacy programme is real.	G-16

7. Findings Register

38 findings identified during the Phase 1 gap assessment. State reflects the position at report date following the evidence review. Severity is assigned from the position of the control and the work required to close it, so an absent control that is expensive to build outranks an absent control that is not.

G/R	Area	Finding	Severity	State	Criterion
G-01	CC6	Recovered data from a disposed laptop or an unattached storage volume is a breach with no attacker required. *First move:* Enforce full disk encryption on every company laptop through MDM and monitor for non-compliant devices.	**High**	**Gap identified**	CC6.5
G-02	P	Decisions made from inaccurate personal data cause real harm, which is exactly what this criterion is about. *First move:* Validate personal data at the point of entry rather than accepting anything.	**High**	**Gap identified**	P7.1
G-03	P	Every privacy criterion after this one is measured against what your notice said you would do. *First move:* Write or refresh the privacy notice covering categories collected, purposes, disclosures, retention, and rights.	**High**	**Gap identified**	P1.1

G/R	Area	Finding	Severity	State	Criterion
G-04	P	The auditor samples real requests and measures your response time against the commitment in your notice. *First move:* Publish one intake channel for access requests and log every request with a received date.	**High**	**Gap identified**	P5.1
G-05	CC2	Controls that run off stale or hand-typed data fail the moment an auditor samples against the source system. *First move:* Build an asset inventory that is generated from your cloud accounts and MDM rather than maintained manually.	**High**	**Gap identified**	CC2.1
G-06	P	Sensitive data attracts higher penalties and higher scrutiny, so the consent bar is deliberately higher. *First move:* Check the personal data inventory for sensitive categories and mark them explicitly.	**High**	**Gap identified**	P3.2
G-07	CC1	Most breaches at this company size start with a person, so the auditor checks whether you hire and train deliberately. *First move:* Add security responsibilities to job descriptions for engineering, IT, and any role handling customer data.	**High**	**Gap identified**	CC1.4
G-08	CC7	The auditor tests whether a consistent, documented judgement was applied rather than case-by-case improvisation. *First move:* Define severity levels with a concrete example of each drawn from your own systems.	**High**	**Gap identified**	CC7.3
G-09	P	Your obligations follow the data, so a vendor with no privacy commitment is an unbounded liability. *First move:* Identify every vendor that receives or can access personal data.	**High**	**Gap identified**	P6.4
G-10	CC9	Your customers hold you responsible for your subprocessors, and so does the auditor. *First move:* Build a vendor inventory including every SaaS tool with access to production or customer data, pulled from expense and SSO data to catch shadow IT.	**Critical**	**Gap identified**	CC9.2

G/R	Area	Finding	Severity	State	Criterion
G-11	CC3	The auditor wants to see that your controls were chosen because of identified risk, not copied from a template. *First move:* Hold a two hour workshop with engineering, ops, and leadership and brainstorm what could go wrong.	Critical	Gap identified	CC3.2
G-12	CC4	A control that nobody tests is a control that has probably been broken for months. *First move:* Enable continuous configuration monitoring across your cloud accounts and route findings to an owner.	Critical	Gap identified	CC4.1
G-13	P	You cannot honour an accounting-of-disclosures request without a record you kept at the time. *First move:* Create a disclosure register for non-routine disclosures with recipient, data, date, purpose, and authoriser.	High	Not assessed	P6.2
G-14	CC3	Fraud risk is called out separately in the criteria, so a register with no insider scenarios reads as incomplete. *First move:* Add explicit fraud and insider misuse scenarios to the risk register.	High	Not assessed	CC3.3
G-15	P	Data minimisation is the cheapest privacy control you have, because data you never collected cannot leak. *First move:* Inventory the personal data fields you collect across product, marketing, and support.	High	Not assessed	P3.1
G-16	P	Regulators and auditors both look at complaint handling as the clearest signal of whether the privacy programme is real. *First move:* Name a privacy owner and publish their contact address in the privacy notice.	Low	Partial	P8.1
G-17	P	You are on the hook for your subprocessor breach, and your clock starts when they tell you. *First move:* Require a specific notification window in every DPA, tighter than your own customer commitment.	Low	Partial	P6.5

G/R	Area	Finding	Severity	State	Criterion
G-18	CC3	Most control failures at growing companies happen right after a change nobody assessed. *First move:* Write a trigger list of change types that force a risk re-assessment.	Low	Partial	CC3.4
G-19	CC2	A policy nobody has read is not a control, and the auditor will ask a random employee how they would report a phishing email. *First move:* Host the full policy set in one place every employee can open, and link it from onboarding.	Low	Partial	CC2.2
G-20	P	The auditor looks for a maintained log, because a period with zero recorded privacy incidents usually means nobody was recording them. *First move:* Add a privacy incident category to your incident process with its own required fields.	Low	Partial	P6.3
G-21	P	Correction rights are only meaningful if the fix reaches every copy you created. *First move:* Add a correction path to the same intake channel as access requests.	Low	Partial	P5.2
G-22	P	A deletion request you cannot evidence to completion is a promise you did not keep. *First move:* Implement hard delete or crypto-shredding for personal data rather than soft delete alone.	Low	Partial	P4.3
G-23	P	This is the criterion that proves your disclosure records are usable, not just stored. *First move:* Write a procedure for assembling a per-individual accounting from your systems and registers.	Low	Partial	P6.7
G-24	P	Purpose creep is the most common privacy finding, and it usually happens without anyone deciding to do it. *First move:* Record the approved purposes per data category and make that list easy for teams to find.	Low	Partial	P4.1

G/R	Area	Finding	Severity	State	Criterion
G-25	CC1	The auditor is checking that security is not self-graded by the only person who would look bad if it were failing. *First move:* Add a standing security and compliance item to the board or advisory meeting agenda, at least quarterly.	Low	Partial	CC1.2
G-26	C1	A deletion promise you cannot demonstrate is a contractual claim your auditor will not sign off on. *First move:* Define a retention period for each data type and record the contractual or legal reason behind it.	Low	Partial	C1.2
G-27	A1	Backups you never verified are the difference between a bad day and losing the company. *First move:* Define what gets backed up, how often, and how long it is retained, tied to your recovery point objective.	Low	Partial	A1.2
G-28	CC7	The auditor is checking that you can return to normal operation on a known timeline rather than hoping. *First move:* Write recovery runbooks for your top scenarios: compromised credential, compromised host, and data corruption.	Low	Partial	CC7.5
G-29	CC6	The auditor is checking that data in motion is protected and that bulk movement is deliberate and logged. *First move:* Require TLS 1.2 or higher for all external connections and disable older protocol versions.	Low	Partial	CC6.7
G-30	CC6	Least privilege is what limits blast radius when one account is eventually compromised. *First move:* Run a documented user access review quarterly across production, cloud, source control, and any system holding customer data.	Low	Partial	CC6.3
G-31	CC5	The auditor tests whether the documented process is the one people actually followed during the period. *First move:* Approve the core policy set with a named owner and an effective date on each document.	Low	Partial	CC5.3

G/R	Area	Finding	Severity	State	Criterion
G-32	CC5	The auditor wants to see design intent, that you chose these controls to address specific identified risks. *First move:* Build a control matrix mapping each significant risk to one or more controls.	Low	Partial	CC5.1
G-33	CC4	The auditor is testing the loop, not the finding: a deficiency you found and closed looks better than one you never had. *First move:* Create a single findings and corrective actions register instead of tracking issues per tool.	Low	Partial	CC4.2
G-34	CC3	Without a written boundary and objective, any risk register is arbitrary and the auditor cannot judge whether you missed something. *First move:* Write a one-page system description: product scope, environments, cloud accounts, data types, and the third parties in the path.	Low	Partial	CC3.1
G-35	CC1	The auditor is testing whether the control owner has any real incentive to run the control on time. *First move:* Put at least one security or compliance objective into the performance review of each named control owner.	Low	Partial	CC1.5
G-36	CC9	The auditor wants to see deliberate choices about disruption, including what you decided to accept. *First move:* Run a business impact analysis listing critical processes with recovery time and recovery point objectives.	Low	Partial	CC9.1
G-37	P	A consent flag with no timestamp or notice version cannot be defended to an auditor or a regulator. *First move:* Map where consent is required versus another lawful basis, and record the decision per processing activity.	Medium	Partial	P2.1
G-38	CC7	The auditor wants proof that alerts were triaged during the period, not just that a monitoring tool was purchased. *First move:* Ship application, infrastructure, and cloud audit logs to one central store with retention of at least one year.	Medium	Partial	CC7.2

Criteria asserted without supporting evidence

These 8 criteria are answered Met or Partial with no artifact collected against them. They are not findings. They are the positions where the only thing on file is an assertion, and they are where an auditor samples first: CC1.2, CC6.4, CC7.5, A1.2, C1.2, P4.1, P6.1, P6.5.

8. Remediation Roadmap

The findings register ordered by the work required to close each entry, which is the order remediation is actually sequenced in. Owner and target are left for Kestrel Data Systems Inc. to assign: a plan carrying our names against your commitments is not a plan anyone is accountable to. Every row below already exists as a tracked item on the remediation board in the portal.

Quick wins, closable within one week (8)

G/R	Action	Owner	Target
G-01	Enforce full disk encryption on every company laptop through MDM and monitor for non-compliant devices.		
G-02	Validate personal data at the point of entry rather than accepting anything.		
G-13	Create a disclosure register for non-routine disclosures with recipient, data, date, purpose, and authoriser.		
G-16	Name a privacy owner and publish their contact address in the privacy notice.		
G-17	Require a specific notification window in every DPA, tighter than your own customer commitment.		
G-18	Write a trigger list of change types that force a risk re-assessment.		
G-19	Host the full policy set in one place every employee can open, and link it from onboarding.		
G-20	Add a privacy incident category to your incident process with its own required fields.		

Moderate lift, closable within one month (25)

G/R	Action	Owner	Target
G-03	Write or refresh the privacy notice covering categories collected, purposes, disclosures, retention, and rights.		
G-04	Publish one intake channel for access requests and log every request with a received date.		
G-05	Build an asset inventory that is generated from your cloud accounts and MDM rather than maintained manually.		
G-06	Check the personal data inventory for sensitive categories and mark them explicitly.		
G-07	Add security responsibilities to job descriptions for engineering, IT, and any role handling customer data.		
G-08	Define severity levels with a concrete example of each drawn from your own systems.		
G-09	Identify every vendor that receives or can access personal data.		
G-14	Add explicit fraud and insider misuse scenarios to the risk register.		
G-15	Inventory the personal data fields you collect across product, marketing, and support.		
G-21	Add a correction path to the same intake channel as access requests.		
G-22	Implement hard delete or crypto-shredding for personal data rather than soft delete alone.		
G-23	Write a procedure for assembling a per-individual accounting from your systems and registers.		
G-24	Record the approved purposes per data category and make that list easy for teams to find.		
G-25	Add a standing security and compliance item to the board or advisory meeting agenda, at least quarterly.		
G-26	Define a retention period for each data type and record the contractual or legal reason behind it.		

G/R	Action	Owner	Target
G-27	Define what gets backed up, how often, and how long it is retained, tied to your recovery point objective.		
G-28	Write recovery runbooks for your top scenarios: compromised credential, compromised host, and data corruption.		
G-29	Require TLS 1.2 or higher for all external connections and disable older protocol versions.		
G-30	Run a documented user access review quarterly across production, cloud, source control, and any system holding customer data.		
G-31	Approve the core policy set with a named owner and an effective date on each document.		
G-32	Build a control matrix mapping each significant risk to one or more controls.		
G-33	Create a single findings and corrective actions register instead of tracking issues per tool.		
G-34	Write a one-page system description: product scope, environments, cloud accounts, data types, and the third parties in the path.		
G-35	Put at least one security or compliance objective into the performance review of each named control owner.		
G-36	Run a business impact analysis listing critical processes with recovery time and recovery point objectives.		

Significant projects requiring planned runway (5)

G/R	Action	Owner	Target
G-10	Build a vendor inventory including every SaaS tool with access to production or customer data, pulled from expense and SSO data to catch shadow IT.		
G-11	Hold a two hour workshop with engineering, ops, and leadership and brainstorm what could go wrong.		
G-12	Enable continuous configuration monitoring across your cloud accounts and route findings to an owner.		

G/R	Action	Owner	Target
G-37	Map where consent is required versus another lawful basis, and record the decision per processing activity.		
G-38	Ship application, infrastructure, and cloud audit logs to one central store with retention of at least one year.		

9. Documentation and Evidence Required

Policies the findings depend on

The written instruments the register above rests on, ordered by the number of open criteria each supports. A policy carrying several criteria warrants drafting first, because a single approved document closes more than one row.

Instrument	Open criteria supported
Internal Privacy Policy	12
Information Security Policy	8
Risk Management Policy	7
Incident Response Plan	5
Secure Disposal Policy	3
Access Control Policy	3
Vendor and Third Party Management Policy	3
Data Processing Agreement Template	3
Data Classification Policy	3
Logging and Monitoring Policy	3
Data Retention and Disposal Policy	3
Backup Policy	3
Security Awareness and Training Policy	2

Instrument	Open criteria supported
Human Resources Security Policy	2
Disaster Recovery Plan	2
Asset Management Policy	2
Audit Logging Standard	2
Encryption Policy	2
Acceptable Use Policy	2
Mobile Device Policy	1
Third Party Access Policy	1
Secure Software Development Policy	1
Change Management Policy	1
Vulnerability Management Policy	1
Business Continuity Plan	1

Artifacts required

The evidence the open criteria require behind them. This is the Phase 2 request list, derived from the findings rather than compiled separately, so no artifact is requested without a criterion that requires it.

Artifact	What it must demonstrate
Asset disposal log	Every device retired in the window with serial, disposal date, wipe method, and verifier name.
Disk encryption compliance report	MDM export showing encryption status for 100 percent of managed devices, dated within the window.
Data quality review record	Results of a periodic check showing duplicates, bounces, and stale records found and cleaned, with dates.
Self-service profile editing	Screenshot of the interface showing which fields a user can update themselves.

Artifact	What it must demonstrate
Published privacy notice	Live page with an effective date, plus the archived prior versions.
Change notification record	The email or in-app message announcing a notice change, with the send date and recipient count.
Data subject request log	Every request in the window with received date, type, verification method, completion date, and outcome.
Access request runbook	The step-by-step procedure naming every system searched and the response deadline.
Asset inventory export	Dated export showing hosts, services, and owners, with a note on how it is generated and how often.
Security metrics dashboard	Screenshot dated within the window, with the underlying data source named.
Sensitive data assessment	Signed determination of which sensitive categories are or are not processed, with the reasoning and date.
Explicit consent capture	Screenshot of the unbundled consent prompt and a sample stored consent record.
Training completion report	Export from the training platform showing every person and their completion date, with the gaps closed before you hand it over.
Background check log	A list of new hires in the window with a check-completed date, not the underlying reports.
Security event log	Chronological record for the window showing each event, the triage decision, who made it, and when.
Severity classification criteria	The section of the incident plan defining severities with examples, with its approval date.
Executed DPAs	Signed agreements for every vendor processing personal data, with the notification timelines visible.
Vendor DPA status tracker	The vendor inventory column showing DPA in place, date signed, and next review.
Vendor inventory with risk tiers	Every vendor with data accessed, tier, owner, last review date, and the assurance artifact held.

Artifact	What it must demonstrate
Vendor assurance reports on file	Current SOC 2 or ISO certificates for critical vendors, with your review notes on any exceptions or carve-outs.
Signed agreements and DPAs	Executed contracts for critical vendors showing the security and notification clauses.
Risk register	Current version showing scores, owners, treatments, and a last-reviewed date inside the audit window.
Risk assessment meeting record	Attendees, date, and what changed as a result.
Penetration test report	Full report with scope, methodology, findings, and dates inside the audit window, plus the retest or remediation note for anything high or critical.
Internal control self-assessment	Completed assessment showing who performed it, when, and which controls were found deficient.
Disclosure register	All non-routine disclosures in the window with recipient, data categories, date, purpose, and authoriser.

A further 46 artifacts follow the same pattern and are enumerated in full on the request list in the portal.

78 of 128 artifacts are collected (61 percent). The register is live in the portal and every item on it maps to the criteria it proves, so collection continues after this report without a new list being written.

10. Timeline and Next Steps into Phase 2

Phase 2 sequences remediation by what unblocks evidence collection rather than strictly by severity, on the reasoning that a control cannot be evidenced until it exists and an auditor samples evidence rather than intent. Controls are rebuilt where the design would not survive sampling, policies are fitted to the systems actually in operation rather than adopted generically, and evidence is collected against the request list until the register is auditor ready.

Every finding in section 7 is already a tracked item on the remediation board with an owner slot and a due date. Phase 2 therefore begins from this register rather than from a fresh discovery exercise, and progress against it is visible to both parties throughout.

Nothing in this report constitutes an audit opinion, a certification, or a representation that the criteria assessed as Met would be accepted by any particular audit firm. It is our assessment of the control set as it stands at the report date, prepared so that the work it implies can be planned, sequenced and priced.