

Paper Tiger Technologies

SOC 2 Control Readiness Workbook

Security, Availability, and Confidentiality — Control Readiness for Demonstration

Document Control

This page records illustrative metadata for this sample workbook. All entries are synthetic.

Field	Value (illustrative)
Document title	Trust Center Control Readiness Workbook
Document owner	Security Program Lead (fictional role)
Version	0.9 (draft, illustrative)
Status	Sample / non-production
Classification	Fictional demo content
Review cadence	Quarterly (illustrative)
Next review	Illustrative date — Q1 of the demo period
Applicable framework	SOC 2 Trust Services Criteria (general concept reference only)

Revision history

Version	Date (illustrative)	Author (fictional role)	Summary
0.7	Demo period — month 1	Security Program Lead	Initial draft assembled
0.8	Demo period — month 2	Security Program Lead	Added procedures and samples
0.9	Demo period — month 3	Security Program Lead	Added test plan and tracker

All version numbers, dates, and roles are illustrative and do not correspond to real events or people.

Purpose and Nature of This Document

This workbook is a fictional, non-production control-readiness artifact. It is not a SOC 2 report, not an audit, not an attestation, and not a certification. It contains no auditor opinion, no seal, no firm branding, and no certification badge. Every control, evidence item, person, date, metric, finding, and sample shown here is illustrative.

The workbook demonstrates, inside a controlled trust-center environment, the kind of control documentation a vendor might assemble. Paper Tiger Technologies and the PaperTiger platform are fictional.

Framework reference (general concept only)

Control areas are organized around the security, availability, and confidentiality categories of the SOC 2 Trust Services Criteria, as those categories are described in general by the American Institute of Certified Public Accountants (AICPA). This is a reference to framework concepts only; no specific or proprietary report language is reproduced.

How to read this workbook

Each section follows a consistent pattern: an objective, an illustrative procedure, acceptance criteria, and the illustrative records that would support the control. Where a table is shown, every value in it is synthetic.

Glossary

All definitions are illustrative and general.

Term	Illustrative meaning
Control readiness	The degree to which a control is designed, documented, and evidenced (illustrative).
Trust Services Criteria	General framework categories for security, availability, processing integrity, confidentiality, and privacy (concept reference only).
Hollow Score	Fictional product concept: an explainable risk score for a vendor.
Facade Scan	Fictional product concept: scanning a vendor's public presence.
RACI	Responsible, Accountable, Consulted, Informed.
RTO / RPO	Recovery time objective / recovery point objective (illustrative values).
Tabletop exercise	A discussion-based walkthrough of a scenario (illustrative).
Subprocessor	A third party supporting the fictional service (illustrative).
Evidence register	A list of illustrative records that support control operation.
Remediation tracker	A list of illustrative findings and their treatment status.
Control environment	The tone, governance, and personnel practices that support controls (illustrative).
Entity-level control	A control that applies across the whole fictional organization (illustrative).

1. System Description

1.1 Overview

PaperTiger is a fictional software-as-a-service platform that helps procurement and third-party risk teams identify vendors whose public presence and claims do not match their substance. The platform collects publicly available information, checks stated claims against public evidence, maps relationships between entities and domains, and produces an explainable risk score. The system description below is entirely illustrative.

1.2 User types (illustrative)

User type	Illustrative description
Customer administrator	Manages the customer's account, users, and watchlists
Customer analyst	Reviews results and works assigned vendor reviews
Internal operator	Operates the fictional platform and supports customers
Internal administrator	Manages platform configuration and access

1.3 Interfaces (illustrative)

- Web application — the primary customer-facing console.
- Reporting API — programmatic retrieval of results.
- Authentication provider — issues and verifies session tokens (illustrative).
- Logging pipeline — receives events from all components.

1.4 Architecture narrative (illustrative)

A customer authenticates through the web console or the reporting API. A set of ingestion services collects public vendor information on a schedule and on demand. That information passes to a scoring engine that produces the Hollow Score, and results are stored for retrieval. Administrative and security events are written to a central log. All component names and behaviors are fictional and do not describe a real product.

1.5 In-scope components (illustrative)

Component	Illustrative purpose
Web application	Customer-facing console for reviewing results and managing watchlists
Ingestion services	Scheduled and on-demand collection of public vendor information
Scoring engine	Processes signals into the Hollow Score
Reporting API	Delivers results to customer systems
Data stores	Configuration, results, and audit-log storage
Logging pipeline	Centralized collection of security and operational events

1.6 Data flows (illustrative)

- Customer authentication flows through the web application and API gateway.
- Public vendor information flows from ingestion services into the scoring engine.
- Results flow from the scoring engine into customer-visible stores.
- Security events flow from all components into the logging pipeline.

1.7 Trust boundary (illustrative)

The trust boundary encloses the web application, ingestion services, scoring engine, reporting API, data stores, and logging pipeline. Customer environments, customer-provided data, and any on-premises components sit outside the boundary and are excluded from this workbook.

2. Scope and Boundaries

2.1 In scope (illustrative)

- The PaperTiger web application, reporting API, ingestion services, and scoring engine.
- The fictional data stores and logging pipeline that support those components.
- The control areas described in this workbook: security, availability, and confidentiality.

2.2 Out of scope (illustrative)

- Customer-managed integrations and customer-provided data beyond the minimum needed for scoring.
- Any on-premises components or customer environments.
- Processing integrity and privacy criteria beyond the confidentiality controls described here.

2.3 Exclusions and limitations (illustrative)

This workbook describes control readiness only. It does not describe actual testing of a real system, and it contains no opinion on whether any control is suitably designed or operating. No real boundaries, systems, or data are represented.

3. Risk Assessment and Risk Register

3.1 Approach (illustrative)

An annual risk assessment reviews threats to confidentiality, availability, and integrity. Each risk is rated for likelihood and impact, assigned an owner, mapped to controls, and given a treatment decision. The register below is entirely synthetic.

3.2 Risk register (illustrative)

ID	Risk description	Category	Likelihood	Impact	Treatment	Key control	Owner
R-01	Unauthorized access to customer result data	Confidentiality	Medium	High	Mitigate	AC-01..AC-04	Security lead
R-02	Regional outage affecting availability	Availability	Low	High	Mitigate	BC-01, BC-02	Platform lead
R-03	Change that degrades scoring accuracy	Availability	Medium	Medium	Mitigate	CH-01..CH-03	Engineering lead
R-04	Unpatched dependency exploited	Security	Medium	High	Mitigate	VM-01, VM-02	Security lead
R-05	Third-party subprocessor incident	Confidentiality	Low	Medium	Mitigate	VMG-01	Security lead
R-06	Administrative credential misuse	Security	Low	High	Mitigate	AC-01, AC-04	Security lead
R-07	Data not deleted on customer request	Confidentiality	Low	Medium	Mitigate	DH-02, DH-03	Data protection lead
R-08	Log tampering or loss	Security	Low	Medium	Mitigate	LM-01, LM-02	Platform lead
R-09	Insider misuse of access	Security	Low	High	Mitigate	AC-02, AC-03	Security lead
R-10	Failed recovery during an outage	Availability	Low	High	Mitigate	BC-01, BC-02	Platform lead
R-11	Vendor claim-check returns false negative	Availability	Medium	Medium	Accept	CH-01	Engineering lead

R-12	Unauthorized disclosure in logs	Confidentiality	Low	Medium	Mitigate	LM-01, DH-01	Security lead
------	---------------------------------	-----------------	-----	--------	----------	--------------	---------------

All risks, ratings, owners, and control references are illustrative.

4. Policy and Control Matrix

The matrix maps illustrative controls to the security, availability, and confidentiality categories. It is a readiness reference only, not a statement of operating effectiveness.

ID	Category	Control description (illustrative)	Owner	Frequency	Evidence
AC-01	Security	Access is granted using unique accounts with multi-factor authentication	Security lead	Continuous	E-01
AC-02	Security	Access is assigned by role using least privilege	Security lead	On change	E-01
AC-03	Security	Access is reviewed quarterly and removed on departure	Security lead	Quarterly	E-01
AC-04	Security	Administrative actions are logged	Platform lead	Continuous	E-04
CH-01	Availability	Changes require review, approval, and testing before deployment	Engineering lead	On change	E-05
CH-02	Availability	Development and production deployment are separated by role	Engineering lead	Continuous	E-05
CH-03	Availability	Emergency changes follow a defined procedure and post-change review	Engineering lead	On change	E-06
VM-01	Security	Infrastructure and dependencies are scanned	Security lead	Continuous	E-07

		for vulnerabilities			
VM-02	Security	Findings are remediated within defined risk-based targets	Security lead	Ongoing	E-07
LM-01	Security	Security and operational logs are centrally collected	Platform lead	Continuous	E-08
LM-02	Security	Alerts are defined for failed authentication and administrative changes	Security lead	Continuous	E-08
IR-01	Security	An incident response plan defines severity levels and roles	Security lead	Annual	E-09
IR-02	Security	Post-incident reviews produce corrective actions	Security lead	On incident	E-09
BC-01	Availability	Backups are taken and recovery procedures are documented	Platform lead	Continuous	E-10
BC-02	Availability	A recovery test is performed at least annually	Platform lead	Annual	E-10
VMG-01	Confidentiality	New vendors are reviewed before use and monitored periodically	Security lead	On change	E-11
DH-01	Confidentiality	Data is classified and encrypted in transit and at rest	Security lead	Continuous	E-12

DH-02	Confidentiality	Retention and deletion are defined and followed	Data protection lead	Continuous	E-13
DH-03	Confidentiality	Only the minimum data needed for scoring is collected	Data protection lead	Continuous	E-13
EC-01	Security	Personnel complete security awareness training	Security lead	Annual	E-14
EC-02	Security	Personnel acknowledge the acceptable-use policy	People operations	On hire	E-14
EC-03	Availability	Service capacity is monitored and reviewed	Platform lead	Continuous	E-15

5. RACI Matrix

The following responsibilities are illustrative. Roles are fictional.

Activity (illustrative)	Security lead	Platform lead	Engineering lead	Data protection lead
Access review	A	R	C	I
Change approval	C	R	A	I
Vulnerability remediation	A	R	R	I
Alert triage	A	R	C	I
Incident response	A	R	C	C
Backup and recovery	C	A	R	I
Vendor review	A	C	C	R
Data retention and deletion	C	C	I	A
Security awareness	A	C	C	I
Capacity review	C	A	R	I

Key: R = Responsible, A = Accountable, C = Consulted, I = Informed. All entries are illustrative.

6. Control Environment and Entity-Level Controls

This section is illustrative and describes no real organization.

6.1 Tone at the top (illustrative)

The fictional organization documents a commitment to security and confidentiality in an information-security policy that leadership reviews annually.

6.2 Personnel practices (illustrative)

- Background checks for personnel before access is granted (illustrative).
- Security awareness training on hire and annually (illustrative).
- Acknowledgment of the acceptable-use policy on hire (illustrative).

6.3 Policy documents index (illustrative)

Policy (illustrative)	Owner	Review cadence
Information Security Policy	Security lead	Annual
Acceptable Use Policy	People operations	Annual
Access Control Policy	Security lead	Annual
Change Management Policy	Engineering lead	Annual
Incident Response Policy	Security lead	Annual
Business Continuity Policy	Platform lead	Annual
Vendor Management Policy	Security lead	Annual
Data Classification and Handling Policy	Data protection lead	Annual
Vulnerability Management Policy	Security lead	Annual
Logging and Monitoring Policy	Platform lead	Annual

7. Detailed Control Procedures

Each procedure below is illustrative and describes no real system or personnel.

7.1 Access Control

Access Control

Purpose (illustrative): To limit access to systems and data to authorized individuals.

Procedure (illustrative):

1. Step 1: Requests for access are submitted with a business justification.
2. Step 2: Access is granted to the minimum role required for the person's duties.
3. Step 3: Multi-factor authentication is enforced for all production access.
4. Step 4: Unique accounts are used; shared administrative credentials are prohibited.
5. Step 5: Access is reviewed quarterly against current duties.
6. Step 6: Departed personnel are removed per the offboarding checklist.
7. Step 7: Service accounts are reviewed and rotated on a defined schedule.
8. Step 8: Exceptions are documented and time-bound.

Acceptance criteria (illustrative): Quarterly review is completed, departed personnel removed, and no undocumented shared credentials exist.

Records (illustrative): Access review records (E-01), offboarding checklist (E-02), MFA enrollment report (E-03).

7.2 Change Management

Change Management

Purpose (illustrative): To ensure changes are reviewed, tested, and deployed in a controlled manner.

Procedure (illustrative):

9. Step 1: A change ticket is created describing the change, testing, and rollback plan.
10. Step 2: The change is peer-reviewed and approved by an independent role.
11. Step 3: The change passes the automated build and test pipeline.
12. Step 4: The change is deployed by a role separate from the developer.
13. Step 5: Post-deployment verification confirms the change behaved as intended.
14. Step 6: The ticket is closed after verification.
15. Step 7: Emergency changes follow a shortened procedure with post-change review.

Acceptance criteria (illustrative): No production change is deployed without an approved ticket and passing tests.

Records (illustrative): Change tickets (E-05), pipeline status (E-06).

7.3 Vulnerability Management

Vulnerability Management

Purpose (illustrative): To identify and remediate vulnerabilities in a timely manner.

Procedure (illustrative):

16. Step 1: Infrastructure and dependencies are scanned on a continuous schedule.
17. Step 2: Findings are triaged by severity and assigned a remediation target.
18. Step 3: Critical findings are remediated within the illustrative 7-day target.
19. Step 4: High and medium findings are remediated within risk-based targets.
20. Step 5: Remediation is verified by rescan.
21. Step 6: The finding is closed in the tracker with evidence.

Acceptance criteria (illustrative): No open critical finding exceeds its remediation target.

Records (illustrative): Scan configuration and findings (E-07).

7.4 Logging and Monitoring

Logging and Monitoring

Purpose (illustrative): To retain and review activity to detect and investigate issues.

Procedure (illustrative):

22. Step 1: Application, system, and security logs are forwarded to a central store.
23. Step 2: Alerts are defined for failed authentication and administrative changes.
24. Step 3: Alerts are reviewed and triaged on a defined schedule.
25. Step 4: Detection rules are tuned based on review.
26. Step 5: Log retention is verified against the illustrative 12-month target.

Acceptance criteria (illustrative): Alerts fire within the defined threshold and logs are retrievable for investigation.

Records (illustrative): Alert configuration (E-08), retention configuration (E-08).

7.5 Incident Response

Incident Response

Purpose (illustrative): To detect, contain, and recover from security incidents consistently.

Procedure (illustrative):

27. Step 1: An event is triaged against defined severity levels.
28. Step 2: The incident is contained and evidence is preserved.
29. Step 3: The affected surface is scoped using logs.
30. Step 4: Affected parties are notified where required.
31. Step 5: A post-incident review identifies corrective actions.

Acceptance criteria (illustrative): Severity is assigned, containment is documented, and corrective actions are tracked.

Records (illustrative): Tabletop notes (E-09).

7.6 Business Continuity

Business Continuity

Purpose (illustrative): To recover critical service functions after a disruption.

Procedure (illustrative):

- 32. Step 1: Backups are taken on a defined schedule.
- 33. Step 2: Recovery procedures are documented with illustrative RTO and RPO.
- 34. Step 3: A recovery test is performed at least annually.
- 35. Step 4: Test results are recorded and gaps are remediated.

Acceptance criteria (illustrative): Recovery procedures are tested annually and restore verifies against the RPO.

Records (illustrative): Backup restore test record (E-10).

7.7 Vendor Management

Vendor Management

Purpose (illustrative): To assess and monitor third parties that support the service.

Procedure (illustrative):

- 36. Step 1: New vendors are reviewed before use.
- 37. Step 2: Contractual security and confidentiality requirements are documented.
- 38. Step 3: The subprocessor list is maintained and published.
- 39. Step 4: Critical vendors are reviewed periodically.

Acceptance criteria (illustrative): No vendor is onboarded without a completed review record.

Records (illustrative): Vendor review record (E-11).

7.8 Data Handling

Data Handling

Purpose (illustrative): To protect customer data through its lifecycle.

Procedure (illustrative):

- 40. Step 1: Data is classified as customer or internal.
- 41. Step 2: Customer data is encrypted in transit and at rest.
- 42. Step 3: Only the minimum data needed for scoring is collected.

43. Step 4: Retention and deletion are applied per the data lifecycle table.

44. Step 5: Deletion requests are completed on schedule.

Acceptance criteria (illustrative): Deletion requests are completed within the defined window.

Records (illustrative): Data classification policy (E-12), retention schedule (E-13).

8. Evidence Register

The following register is entirely illustrative. Entries, owners, and dates are synthetic.

ID	Evidence item	Illustrative period/date	Illustrative owner
E-01	Access review record	Quarterly	Security lead
E-02	Offboarding checklist	On change	People operations
E-03	MFA enrollment report	Monthly	Security lead
E-04	Administrative-action log sample	Daily	Platform engineering
E-05	Change ticket with approval	On change	Engineering lead
E-06	Deployment pipeline status	Continuous	Platform engineering
E-07	Vulnerability scan and findings	Continuous	Security lead
E-08	Alert and retention configuration	Current	Security lead
E-09	Tabletop exercise notes	Demo period	Security lead
E-10	Backup restore test record	Annual	Platform engineering
E-11	Vendor review record	On change	Security lead
E-12	Data classification policy	Current	Security lead
E-13	Retention and deletion schedule	Current	Data protection
E-14	Security awareness completion	Annual	People operations
E-15	Capacity review record	Monthly	Platform lead

All entries are synthetic and do not correspond to real documents.

8.1 Filled evidence samples

8.1.1 Access review log (sample)

User (fictional)	Role	Last review (illustrative)	Result	Action
user.alpha@example.invalid	Administrator	Demo quarter	Appropriate	No change
user.beta@example.invalid	Analyst	Demo quarter	Appropriate	No change
user.gamma@example.invalid	Engineer	Demo quarter	Excess access	Downgraded

All usernames and domains are fictional placeholders.

8.1.2 Administrative-action log sample (illustrative)

Timestamp (illustrative)	Actor (fictional)	Action	Result
Demo period — 09:12	svc-reporting	Rotate credential	Success

Demo period — 11:40	user.alpha	Grant analyst role	Approved
Demo period — 16:05	user.delta	Revoke access	Success

8.1.3 Vendor review record (illustrative)

Field	Illustrative entry
Vendor name	Fictional Infrastructure Provider
Service provided	Cloud hosting (illustrative)
Data processed	None (hosting only, illustrative)
Security review	Completed before onboarding (illustrative)
Review cadence	Annual (illustrative)

9. Change Tickets (Samples)

These change tickets are illustrative and describe no real change.

Field	Value (illustrative)
Ticket ID	CH-1042
Title	Update scoring rule weight for domain age
Requester	Engineering lead (fictional)
Approver	Security lead (fictional)
Testing	Automated regression suite passed
Rollback plan	Re-deploy prior version
Status	Closed after verification

Field	Value (illustrative)
Ticket ID	CH-1043
Title	Rotate logging-service credential
Requester	Platform lead (fictional)
Approver	Security lead (fictional)
Testing	Credential verified in staging
Rollback plan	Restore prior credential
Status	Closed after verification

All ticket IDs, titles, and roles are synthetic.

10. Access Review Samples

The samples below illustrate the structure and content of a quarterly access review. They are fictional.

10.1 Review scope (illustrative)

- Production application and infrastructure access.
- Administrative and privileged roles.
- Service accounts and API credentials.

10.2 Review findings (illustrative)

Account (fictional)	Finding	Disposition
svc-reporting	Credential not rotated	Rotated and logged
user.delta	Departed personnel	Access revoked
user.epsilon	Role too broad	Reduced to analyst

11. Incident Response Tabletop Scenarios

These are fictional, discussion-based scenarios. No real incident or system is described.

11.1 Scenario A — credential-stuffing attempt

An unauthorized party is reported to be attempting repeated logins against a customer account using credentials obtained elsewhere. The scenario walks the fictional response team through detection, containment, and recovery.

Time (illustrative)	Inject	Expected response
T+0	Alert: burst of failed logins	Security lead triages and confirms
T+15m	Account locked, session terminated	Platform lead confirms containment
T+1h	Logs reviewed for scope	Security lead documents affected surface
T+4h	Customer notified	Notification drafted per plan
T+1d	Post-incident review	Corrective actions recorded

11.2 Scenario B — unauthorized administrative action

A change to an administrative role is detected outside the change-management process. The fictional team walks through containment, scoping, and remediation.

Time (illustrative)	Inject	Expected response
T+0	Alert: administrative change without ticket	Platform lead confirms and freezes change
T+30m	Affected role and session identified	Security lead revokes and resets
T+2h	Scope confirmed from logs	Security lead documents
T+1d	Change ticket opened retroactively	Engineering lead reviews

11.3 Lessons (illustrative)

- Detection worked as designed; alerts fired within threshold.
- Notification wording should be pre-approved to reduce delay.
- Add a step to reset the affected customer's API credentials.

12. Business Continuity / Disaster Recovery Tabletop

These are fictional, discussion-based scenarios. No real outage is described.

12.1 Scenario A — regional zone unavailable

A regional infrastructure zone is reported unavailable. The fictional team walks through failing over to a second zone and restoring from backup.

Phase	Illustrative action	Illustrative target
Detect	Monitoring alerts on the affected zone	Within minutes
Decide	Declare the incident and authorize failover	Within 30 minutes
Fail over	Route traffic to the second zone	Within RTO of 24 hours
Restore	Verify data against RPO of 1 hour	After failover
Review	Document gaps and update the plan	Within one week

12.2 Scenario B — backup restore verification

A sample of customer result data is restored from backup to verify integrity and the recovery procedure.

- Restore a defined sample of result data.
- Verify checksums and record completeness.
- Confirm the restore completed within the illustrative RTO.
- Record observations and any gaps.

12.3 Outcomes (illustrative)

- Failover procedure was followed and verified.
- Observation: the runbook should include a pre-check of the second zone's capacity.

13. Vendor Assessment Template

This template is illustrative and contains no real vendor.

Field	Illustrative entry
Vendor name	Fictional Infrastructure Provider
Service provided	Cloud hosting (illustrative)
Data processed	None (hosting only, illustrative)
Security review	Completed before onboarding (illustrative)
Contractual controls	Confidentiality and security terms in place (illustrative)
Review cadence	Annual (illustrative)
Risk rating	Low (illustrative)

14. Vulnerability Remediation Examples

These examples are illustrative and describe no real vulnerability.

14.1 Example A (critical, illustrative)

- Finding: dependency with a known remote-code-execution issue.
- Action: patched within the illustrative 7-day target.
- Verification: rescan confirmed the finding was resolved.

14.2 Example B (medium, illustrative)

- Finding: overly permissive default role on a staging environment.
- Action: role reduced to least privilege within 30 days.
- Verification: access review confirmed the change.

14.3 Example C (low, illustrative)

- Finding: missing reminder cadence for medium findings.
- Action: cadence added to the tracker.
- Verification: quarterly review confirmed the reminder.

15. Logging and Monitoring Scenarios

These scenarios are illustrative and describe no real events.

15.1 Scenario A: failed authentication burst

Repeated failed logins against a single account raise an alert within the defined threshold. The alert includes the account, source, and timestamp.

15.2 Scenario B: administrative change

A change to an administrative role raises an alert and is recorded in the administrative-action log for later review.

15.3 Scenario C: retention verification

A sample of logs is confirmed to be retained for the illustrative 12-month period and is retrievable for investigation.

15.4 Scenario D: log tampering

An attempt to modify a security log is detected and raises an alert; the original event is preserved in a write-once store (illustrative).

16. Data Lifecycle Table

This table is illustrative and describes no real data.

Data type (illustrative)	Classification	Collected	Retention	Deletion
Customer account details	Customer	At signup	For the life of the account	On account closure
Vendor public information	Public	At scan	12 months (illustrative)	Per schedule
Scoring results	Customer	At scan	12 months (illustrative)	Per schedule
Security logs	Internal	Continuous	12 months (illustrative)	Per schedule
Authentication events	Internal	Continuous	12 months (illustrative)	Per schedule
Alert history	Internal	Continuous	12 months (illustrative)	Per schedule

17. Test Plan

This test plan is illustrative and describes no real testing.

Test ID	Control area	Test description (illustrative)	Frequency
TP-01	Access control	Provision and remove a test account; verify revocation	Quarterly
TP-02	Change management	Attempt a production change without approval; verify block	Quarterly
TP-03	Vulnerability management	Confirm findings appear in the tracker with targets	Continuous
TP-04	Logging/monitoring	Generate failed logins; confirm alert	Quarterly
TP-05	Business continuity	Restore sample data from backup and verify	Annual
TP-06	Incident response	Walk through a synthetic exposure scenario	Annual
TP-07	Data handling	Verify a deletion request completes on schedule	Quarterly
TP-08	Vendor management	Confirm a sample vendor has a completed review record	Annual
TP-09	Control environment	Confirm awareness-training completion for a sample of users	Annual
TP-10	Capacity	Review capacity metrics against thresholds	Monthly

18. Findings and Remediation Tracker

This tracker is illustrative and contains no real findings.

Finding ID	Source	Description (illustrative)	Severity	Owner	Status	Target
F-01	TP-03	Reminder cadence for medium findings is missing	Low	Security lead	Open	30 days
F-02	TP-06	Notification wording not pre-approved	Low	Security lead	Open	14 days
F-03	TP-05	Runbook lacks second-zone capacity pre-check	Low	Platform lead	Open	30 days
F-04	TP-04	Alert tuning for one rule	Low	Security lead	Closed	Done
F-05	TP-08	One vendor record missing review date	Low	Security lead	Open	7 days

19. Annual Control Calendar

This calendar is illustrative and describes no real schedule.

Month (illustrative)	Control activity
Q1	Annual risk assessment; access review; awareness training refresh
Q2	Access review; business-continuity recovery test; capacity review
Q3	Access review; incident-response tabletop; vendor review
Q4	Access review; penetration-test planning (illustrative); policy review

Appendix A. Control-to-Criteria Mapping

This appendix maps illustrative controls to the general framework categories. It is a reference only and is not an assertion of conformance.

Category (illustrative)	Illustrative controls
Security	AC-01..AC-04, VM-01..VM-02, LM-01..LM-02, IR-01..IR-02, EC-01..EC-02
Availability	CH-01..CH-03, BC-01..BC-02, EC-03
Confidentiality	VMG-01, DH-01..DH-03

20. Additional Detailed Evidence Samples

This section provides twelve additional filled evidence templates. Every value, name, date, identifier, and metric is illustrative and synthetic; none describes a real system, person, or event.

20.1 Sample S-01: Quarterly access review (filled)

Field	Value (illustrative)
Review period	Q2 2026 (illustrative)
Review owner	Security lead (illustrative)
Accounts reviewed	214 service and human accounts (illustrative)
High-privilege accounts	9 (illustrative)
Removals	3 stale accounts revoked (illustrative)
Exceptions	1 documented with owner approval (illustrative)
Review date	2026-06-30 (illustrative)

20.2 Sample S-02: Onboarding and offboarding checklist (filled)

Step (illustrative)	Recorded result (illustrative)
Identity verified	Yes, via documented procedure (illustrative)
Role assigned	Least-privilege role RB-04 (illustrative)
MFA enrolled	Yes (illustrative)
Access date	2026-05-11 (illustrative)
Revocation on exit	Same business day (illustrative)
Manager confirmation	Recorded (illustrative)

20.3 Sample S-03: Multi-factor authentication configuration summary

Setting (illustrative)	Value (illustrative)
Enforcement	Required for all human accounts (illustrative)
Methods	Hardware token or authenticator app (illustrative)
Fallback	None (illustrative)
Coverage	100% of human accounts (illustrative)
Reviewed	Quarterly (illustrative)

20.4 Sample S-04: Standard change ticket (filled)

Field	Value (illustrative)
Ticket ID	CHG-2026-0117 (illustrative)
Summary	Rotate a service certificate (illustrative)
Requester	Platform engineer (illustrative)
Approver	Change manager (illustrative)
Peer review	1 of 2 (illustrative)
Rollback plan	Recorded (illustrative)
Status	Implemented (illustrative)

20.5 Sample S-05: Emergency change ticket (filled)

Field	Value (illustrative)
Ticket ID	ECHG-2026-0041 (illustrative)
Summary	Restore a failed queue (illustrative)

Reason	Service impairment (illustrative)
Post-hoc approval	Within 24 hours (illustrative)
Review	Completed (illustrative)

20.6 Sample S-06: Vulnerability scan summary excerpt

Field	Value (illustrative)
Scan target	Customer portal tier (illustrative)
Scan date	2026-06-12 (illustrative)
Findings	2 medium, 0 high (illustrative)
Scanner	Internal scanner (name omitted) (illustrative)
Remediation target	Medium within 30 days (illustrative)

20.7 Sample S-07: Alert tuning record (filled)

Field	Value (illustrative)
Rule	Excessive failed logins (illustrative)
Change	Raised threshold after review (illustrative)
Rationale	Legitimate burst traffic (illustrative)
Approver	Security lead (illustrative)
Date	2026-04-02 (illustrative)

20.8 Sample S-08: Incident log entry (filled)

Field	Value (illustrative)
Incident ID	INC-2026-0019 (illustrative)
Type	Synthetic account-takeover drill (illustrative)
Detected	2026-02-09 (illustrative)
Severity	Medium (illustrative)
Contained	Same day (illustrative)
Closed	2026-02-11 (illustrative)

20.9 Sample S-09: Post-incident review summary (filled)

Field	Value (illustrative)
Review date	2026-02-14 (illustrative)
Attendees	Security, platform, support (illustrative)
Actions	3 (illustrative)
Owner	Security lead (illustrative)
Tracking	Findings F-06..F-08 (illustrative)

20.10 Sample S-10: Backup restore test record (filled)

Field	Value (illustrative)
Test date	2026-03-20 (illustrative)
Scope	Sample customer data (illustrative)
Result	Restored and verified (illustrative)
RTO met	Yes (illustrative)
Tester	Platform lead (illustrative)

20.11 Sample S-11: Vendor onboarding due-diligence record (filled)

Field	Value (illustrative)
-------	----------------------

Vendor	V-014 (illustrative)
Review date	2026-05-06 (illustrative)
Checklist	10 of 10 items (illustrative)
Residual risk	Low (illustrative)
Approver	Security lead (illustrative)

20.12 Sample S-12: Data deletion request record (filled)

Field	Value (illustrative)
Request ID	DEL-2026-0027 (illustrative)
Subject	Test account data (illustrative)
Received	2026-06-01 (illustrative)
Completed	2026-06-01 (illustrative)
Verification	Retained no records (illustrative)

21. Expanded System and Dataflow Narrative

This narrative expands the system description in Section 1. All components, zones, flows, and figures are illustrative and describe no real infrastructure.

21.1 Processing stages

The PaperTiger platform is described here as a logical pipeline of six stages. Each stage is a named, illustrative function rather than a real system.

Stage (illustrative)	Description (illustrative)
Collect	Gather vendor public presence, registrations, and documents from configured sources.
Normalize	Convert records to a common schema and drop duplicate or malformed entries.
Enrich	Link records to domains, entities, and documents using the linkage graph.
Score	Apply the Hollow Score model and produce an explainable result per vendor.
Alert	Raise watchlist items and route high-risk results to reviewers.
Retain	Store results and logs according to the illustrative retention schedule.

21.2 Illustrative dataflow

- Customer credentials are authenticated at the edge before any request reaches an internal zone.
- Scan jobs are queued and processed by workers that read only configured, public sources.
- Normalized records are written to a working store and enriched with linkage data.
- Scoring results are written to the customer-visible result store, never back into the source.
- Alerts are emitted to the monitoring pipeline and mirrored to the customer notification channel.
- Retention and deletion are applied by scheduled jobs that reference the data lifecycle table.

21.3 Trust boundary and zones

Zone (illustrative)	Contains (illustrative)	Reachability (illustrative)
Edge	Web, API gateway, authentication	Public
Application	Scoring service, result API	Private
Processing	Collection and enrichment workers	Private, egress to public sources only
Data	Working and result stores, logs	Private
Operations	Alerting, backups, retention jobs	Private

21.4 Interfaces

- Customer portal (web) for viewing scores, evidence, and watchlist items.
- Result API for customer tooling integration (illustrative).
- Single sign-on federation for customer identity providers (illustrative).
- Scheduled export of results and audit records (illustrative).

22. Additional Control Test Procedures

Six additional step-by-step control test procedures. All steps, thresholds, and results are illustrative and describe no real testing.

22.1 AP-01: Access provisioning and revocation

Objective (illustrative): Confirm access is granted by least-privilege role and removed on exit.

Procedure steps (illustrative):

1. Select a sample of newly onboarded accounts and confirm each maps to a documented role.
2. Confirm each account shows an enrolled second factor before first use.
3. Select a sample of departed accounts and confirm revocation within the same business day.
4. Confirm high-privilege accounts require an additional approval.

Acceptance criteria (illustrative): All sampled accounts match their documented role and show timely revocation.

22.2 AP-02: Change management segregation of duties

Objective (illustrative): Confirm a change cannot be implemented by its own requester without independent approval.

Procedure steps (illustrative):

1. Select a sample of production changes.
2. Confirm requester and approver differ for each selected change.
3. Confirm an emergency change that skipped approval received post-hoc review within 24 hours.
4. Confirm a rollback plan exists for each selected change.

Acceptance criteria (illustrative): No selected change shows requester and approver as the same person without documented review.

22.3 AP-03: Vulnerability remediation against targets

Objective (illustrative): Confirm findings are remediated within the illustrative service-level targets.

Procedure steps (illustrative):

1. Select a sample of closed findings.
2. Confirm each has a recorded discovery date and remediation date.
3. Confirm the interval is within the target for the finding severity.
4. Confirm each finding has a verification note after remediation.

Acceptance criteria (illustrative): Sampled findings fall within the illustrative remediation targets.

22.4 AP-04: Log integrity and retention

Objective (illustrative): Confirm logs are retained and protected from modification.

Procedure steps (illustrative):

1. Select a sample of security logs.
2. Confirm each falls within the illustrative retention window.
3. Confirm write-once storage is referenced for high-value logs.
4. Attempt an illustrative modification and confirm an alert is raised.

Acceptance criteria (illustrative): Sampled logs are retrievable and modification attempts are flagged.

22.5 AP-05: Incident notification timing

Objective (illustrative): Confirm notification drafting and approval are timely in a drill.

Procedure steps (illustrative):

1. Run a synthetic incident and record detection time.
2. Record when the notification draft is first produced.
3. Confirm approval and dispatch occur within the illustrative window.
4. Confirm the post-incident review is scheduled.

Acceptance criteria (illustrative): The drill meets the illustrative notification window.

22.6 AP-06: Backup encryption and restore

Objective (illustrative): Confirm backups are encrypted and restorable.

Procedure steps (illustrative):

1. Select a sample backup set.
2. Confirm the backup is encrypted at rest (illustrative).
3. Restore the sample to a sandbox and verify integrity.
4. Confirm the restore time is within the illustrative recovery objective.

Acceptance criteria (illustrative): The sample restores successfully within the illustrative objective.

23. Additional Incident and Business-Continuity Tabletop Scenarios

Four additional tabletop scenarios. All participants, injects, timelines, and outcomes are illustrative and synthetic.

23.1 IR-03: Synthetic account takeover

Objective (illustrative): Exercise detection, containment, and user notification for an account compromise.

Participants (illustrative): Security lead, platform lead, support lead.

Injects (illustrative):

Time (illustrative)	Inject (illustrative)
T+0	Alert on impossible-travel logins from a test account.
T+10	Account is disabled and sessions revoked.
T+30	Affected user is notified; review of the account's actions begins.

Outcome (illustrative): Contained within the window; one finding recorded about alert wording.

23.2 IR-04: Synthetic mishandled export

Objective (illustrative): Exercise the response to an export sent to the wrong illustrative recipient.

Participants (illustrative): Security lead, support lead, data lead.

Injects (illustrative):

Time (illustrative)	Inject (illustrative)
T+0	Support reports a file sent to the wrong address.
T+15	Recipient access is assessed and the file is revoked.
T+45	Notification decision is recorded and approved.

Outcome (illustrative): No sensitive data confirmed exposed; process note added for export checks.

23.3 BC-03: Primary zone outage

Objective (illustrative): Exercise failover when the primary application zone is unavailable.

Participants (illustrative): Platform lead, operations lead, support lead.

Injects (illustrative):

Time (illustrative)	Inject (illustrative)
T+0	Primary zone becomes unreachable (illustrative).
T+20	Traffic is shifted to the secondary zone.
T+40	Result API and portal are verified healthy.

Outcome (illustrative): Service restored within the illustrative recovery objective.

23.4 BC-04: Synthetic encryption event containment

Objective (illustrative): Exercise containment of a suspected encryption event in a sandbox.

Participants (illustrative): Security lead, platform lead, operations lead.

Injects (illustrative):

Time (illustrative)	Inject (illustrative)
T+0	Sandbox host shows unexpected file changes (illustrative).
T+10	Host is isolated and credentials rotated.
T+30	Restore from backup is verified in a clean sandbox.

Outcome (illustrative): Contained in the sandbox; backup restore verified; no production impact.

24. Vendor-Risk Case Files

Six vendor-risk case files. Every vendor, finding, and rating is illustrative and synthetic; none refers to a real organization.

24.1 VR-01: Registration anomaly

Field	Value (illustrative)
Vendor	V-101 (illustrative)
Signal	Head-office address shared by many unrelated entities
Category	Shell / facade
Hollow Score	Elevated
Disposition	Referred for deeper check

24.2 VR-02: Borrowed attestation

Field	Value (illustrative)
Vendor	V-102 (illustrative)
Signal	Stated certification belongs to a similarly named entity
Category	Claim mismatch
Hollow Score	High
Disposition	Onboarding paused

24.3 VR-03: Cloned domain

Field	Value (illustrative)
Vendor	V-103 (illustrative)
Signal	Domain registered days ago and mirroring a known site
Category	Impersonation
Hollow Score	High
Disposition	Blocked and reported internally

24.4 VR-04: High subprocessor count

Field	Value (illustrative)
Vendor	V-104 (illustrative)
Signal	Unusually large, shifting subprocessor list
Category	Supply-chain opacity
Hollow Score	Medium
Disposition	Requested a complete list

24.5 VR-05: Single-threaded critical service

Field	Value (illustrative)
Vendor	V-105 (illustrative)
Signal	Critical service depends on one person
Category	Availability concentration
Hollow Score	Medium
Disposition	Continuity plan requested

24.6 VR-06: Data-residency ambiguity

Field	Value (illustrative)
Vendor	V-106 (illustrative)
Signal	Conflicting statements about where data is stored
Category	Confidentiality
Hollow Score	Medium
Disposition	Clarification requested

25. Vulnerability and Remediation Case Files

Six vulnerability and remediation case files. Every finding, severity, timeline, and remediation is illustrative and synthetic.

25.1 VU-01: Outdated library in report export

Field	Value (illustrative)
Finding	Outdated parsing library (illustrative)
Severity	Medium
Discovered	2026-01-15 (illustrative)
Remediated	2026-01-28 (illustrative)
Verification	Re-scan clean (illustrative)

25.2 VU-02: Missing security header on a legacy endpoint

Field	Value (illustrative)
Finding	Missing response header (illustrative)
Severity	Low
Discovered	2026-02-03 (illustrative)
Remediated	2026-02-05 (illustrative)
Verification	Header confirmed (illustrative)

25.3 VU-03: Overly permissive role

Field	Value (illustrative)
Finding	Role granted more access than needed (illustrative)
Severity	Medium
Discovered	2026-03-11 (illustrative)
Remediated	2026-03-14 (illustrative)
Verification	Least privilege restored (illustrative)

25.4 VU-04: Unencrypted legacy snapshot

Field	Value (illustrative)
Finding	Legacy snapshot stored unencrypted (illustrative)
Severity	Medium
Discovered	2026-04-09 (illustrative)
Remediated	2026-04-10 (illustrative)
Verification	Encryption confirmed (illustrative)

25.5 VU-05: Rate-limit gap on an API

Field	Value (illustrative)
Finding	Rate limit missing on one endpoint (illustrative)
Severity	Medium
Discovered	2026-05-07 (illustrative)
Remediated	2026-05-12 (illustrative)
Verification	Limit enforced (illustrative)

25.6 VU-06: Dependency with a known advisory

Field	Value (illustrative)
Finding	Dependency with a published advisory (illustrative)
Severity	Medium
Discovered	2026-06-01 (illustrative)
Remediated	2026-06-03 (illustrative)
Verification	Version pinned (illustrative)

Appendix B. Procedure-to-Evidence Cross-Reference

This appendix links illustrative procedures to the evidence they produce or consume. It is a reference only and asserts nothing.

Procedure (illustrative)	Related evidence (illustrative)
AP-01 Access provisioning	S-02 onboarding checklist, S-01 access review
AP-02 Change management	S-04 change ticket, S-05 emergency change ticket
AP-03 Vulnerability remediation	S-06 scan summary, VU-01..VU-06 case files
AP-04 Log integrity	S-07 alert tuning, S-08 incident log
AP-05 Incident notification	S-08 incident log, S-09 post-incident review
AP-06 Backup restore	S-10 backup restore record
TP-08 Vendor management	S-11 vendor due-diligence record
TP-07 Data handling	S-12 deletion request record

Appendix C. Evidence-to-Procedure Cross-Reference

This appendix maps illustrative evidence to the procedures that consume it, the owner, and the retention. It is a reference only.

Evidence (illustrative)	Consumed by (illustrative)	Owner (illustrative)	Retention (illustrative)
S-01 access review	AP-01, TP-01	Security lead	12 months
S-02 onboarding checklist	AP-01	Security lead	12 months
S-03 MFA summary	AP-01	Security lead	12 months
S-04 change ticket	AP-02, TP-02	Platform lead	12 months
S-05 emergency change ticket	AP-02	Platform lead	12 months
S-06 scan summary	AP-03, TP-03	Security lead	12 months
S-07 alert tuning	AP-04, TP-04	Security lead	12 months
S-08 incident log	AP-05, TP-06	Security lead	12 months
S-09 post-incident review	AP-05	Security lead	12 months
S-10 backup restore	AP-06, TP-05	Platform lead	12 months
S-11 vendor due-diligence	TP-08	Security lead	12 months
S-12 deletion request	TP-07	Data lead	12 months

26. Roles and Responsibilities

The illustrative roles below carry accountability for the control areas in this workbook. All names are omitted; roles only.

26.1 Role descriptions

Role (illustrative)	Accountabilities (illustrative)
Security lead	Access control, vulnerability management, logging, incident response, vendor review
Platform lead	Change management, capacity, business continuity, backups
Data lead	Data classification, handling, retention, deletion
Support lead	First-line triage, customer notification support
Compliance lead	Policy maintenance, control testing coordination, training
Executive sponsor	Risk acceptance, resource approval, tone at the top

26.2 Segregation of duties

- The person who requests a production change is not the sole approver of that change.
- The person who grants access is not the only person who reviews that access.
- Incident severity is set by one role and independently reviewed by a second.

26.3 Succession and coverage

Each control owner has a named alternate (illustrative) so no single control depends on one person. Coverage is reviewed during the annual control calendar (illustrative).

27. Metrics and Reporting

The metrics below are illustrative. Thresholds and values describe no real system.

27.1 Key indicators

Metric (illustrative)	Definition (illustrative)	Target (illustrative)	Frequency	Owner
Access review completion	Accounts reviewed within the period	100%	Quarterly	Security lead
Privileged access count	Active high-privilege accounts	<= 10	Monthly	Security lead
Vulnerability remediation	Findings closed within target	>= 95%	Monthly	Security lead
Backup restore success	Restore tests passing	100%	Annual	Platform lead
Incident time to contain	Detection to containment	Within window	Per event	Security lead
Training completion	Users completing annual training	100%	Annual	Compliance lead

27.2 Reporting cadence

- Operational metrics are reviewed monthly by the control owners.
- Control testing results are compiled quarterly.
- A risk summary is presented to the executive sponsor annually.

27.3 Escalation

A metric missing its target for two consecutive periods is escalated to the compliance lead and logged as an exception or finding (illustrative).

28. Training and Awareness Program

This program is illustrative and describes no real training or real people.

28.1 Program description

All personnel with access to the platform complete annual security and privacy awareness training (illustrative). Role-specific training is assigned to security, platform, and data personnel. Completion is recorded and reviewed annually.

28.2 Annual plan

Topic (illustrative)	Audience (illustrative)	Cadence
Security and privacy awareness	All personnel	Annual
Incident response roles and duties	On-call personnel	Annual
Secure change management	Platform personnel	Annual
Data handling and classification	All personnel	Annual
Vendor due diligence	Security and compliance personnel	Annual

28.3 Sample training log (illustrative)

Session (illustrative)	Date (illustrative)	Completion
Security awareness	2026-01-20	100%
Incident response	2026-02-15	100%
Data handling	2026-03-10	100%

29. Policy Documents Index

The policies below are illustrative. Titles, owners, and cadences describe no real documents.

Policy ID (illustrative)	Title (illustrative)	Purpose (illustrative)	Owner	Review
POL-01	Information Security Policy	Sets the security program and controls	Security lead	Annual
POL-02	Access Control Policy	Defines access, authentication, and review	Security lead	Annual
POL-03	Change Management Policy	Defines change types, approval, rollback	Platform lead	Annual
POL-04	Vulnerability Management Policy	Sets scanning, prioritization, remediation	Security lead	Annual
POL-05	Incident Response Policy	Defines severity, roles, notification	Security lead	Annual
POL-06	Business Continuity Policy	Sets recovery objectives and testing	Platform lead	Annual
POL-07	Vendor Management Policy	Sets due diligence and monitoring	Security lead	Annual
POL-08	Data Classification and Handling Policy	Defines labels and handling rules	Data lead	Annual
POL-09	Logging and Monitoring Policy	Defines collection, retention, alerting	Security lead	Annual
POL-10	Acceptable Use Policy	Sets personnel responsibilities	Compliance lead	Annual
POL-11	Remote Work Policy	Sets device and connection expectations	Security lead	Annual
POL-12	Privacy Notice	Describes data collection and use	Compliance lead	Annual

30. Control Testing and Monitoring Schedule

This schedule maps illustrative control areas to testing and monitoring cadences.

Control area (illustrative)	Test / monitor (illustrative)	Frequency	Owner	Evidence
Access control	Provisioning and revocation test	Quarterly	Security lead	S-01, S-02
Access control	Quarterly access review	Quarterly	Security lead	S-01
Change management	Segregation-of-duties test	Quarterly	Platform lead	S-04, S-05
Vulnerability management	Remediation SLA review	Monthly	Security lead	S-06
Logging/monitoring	Alert generation test	Quarterly	Security lead	S-07, S-08
Incident response	Tabletop exercise	Annual	Security lead	S-08, S-09
Business continuity	Backup restore test	Annual	Platform lead	S-10
Vendor management	Due-diligence review	Annual	Security lead	S-11
Data handling	Deletion request verification	Quarterly	Data lead	S-12
Control environment	Training completion review	Annual	Compliance lead	Training log

31. Third-Party and Subprocessor Register

The subprocessors below are illustrative and synthetic; none is a real organization.

Subprocessor (illustrative)	Service (illustrative)	Data (illustrative)	Review (illustrative)
SP-01 Cloud host	Infrastructure hosting	Customer and platform data	2026-01-10
SP-02 Analytics provider	Product usage analytics	De-identified usage	2026-02-14
SP-03 Messaging provider	Notification delivery	Notification content	2026-03-05
SP-04 Support tool	Ticket management	Support metadata	2026-04-12
SP-05 Backup provider	Encrypted offsite backups	Encrypted platform data	2026-05-08
SP-06 Identity provider	Single sign-on	Authentication events	2026-06-02

31.1 Due diligence

- Each subprocessor is reviewed against the vendor checklist before engagement (illustrative).
- The register is reviewed at least annually and updated on change (illustrative).
- No subprocessor processes more data than its service requires (illustrative).

32. Asset and Configuration Inventory

Asset classes below are illustrative and describe no real hardware or software.

Asset class (illustrative)	Examples (illustrative)	Owner	Classification
Production workloads	Application and scoring services	Platform lead	Internal
Data stores	Result store, working store, logs	Data lead	Internal
End-user devices	Managed workstations	Security lead	Internal
Secrets	Keys, tokens, certificates	Security lead	Internal
Source code	Repositories and build artifacts	Platform lead	Internal
Network devices	Gateways and firewalls	Security lead	Internal

32.1 Inventory maintenance

The inventory is updated on change and reconciled quarterly (illustrative). Every asset has an owner and a classification, and secrets are stored separately from code (illustrative).

33. Network and Environment Description

This description is illustrative and expands the trust boundary in Sections 1 and 21.

33.1 Environments

Environment (illustrative)	Purpose (illustrative)
Production	Customer-facing platform and data
Staging	Pre-release validation with synthetic data
Development	Build and unit testing
Sandbox	Tabletop and restore testing

33.2 Segmentation

- Production is segmented from staging, development, and sandbox (illustrative).
- Only the edge zone is reachable from the public internet (illustrative).
- Administrative access uses a dedicated channel with multi-factor authentication (illustrative).
- Staging and sandbox use synthetic data only (illustrative).

33.3 Configuration baseline

A documented baseline is applied to all environments, and drift is reviewed monthly (illustrative).

34. Data Classification and Handling Guide

This guide is illustrative and describes no real data.

Classification (illustrative)	Examples (illustrative)	Handling (illustrative)
Customer	Account details, scoring results	Encrypted in transit and at rest; least privilege
Internal	Security logs, runbooks	Role-based access; retained per schedule
Public	Published documentation	No special handling

34.1 Handling rules

- Customer data is encrypted in transit and at rest (illustrative).
- Access to customer data is logged and reviewed (illustrative).
- Data is deleted according to the lifecycle table on request (illustrative).
- Synthetic data is used in all non-production environments (illustrative).

35. Exception Management and Tracking

Exceptions are documented, risk-assessed, approved, and time-boxed. All entries are illustrative.

35.1 Exception log (illustrative)

Exception ID	Control (illustrative)	Description (illustrative)	Approver	Expires
EX-01	Access review	One stale account retained pending owner review	Executive sponsor	30 days
EX-02	Change management	Emergency change approved post-hoc	Platform lead	Closed
EX-03	Vendor review	One vendor review postponed one quarter	Security lead	90 days

35.2 Process

- An exception is logged with a description, risk assessment, and approver.
- Exceptions expire and must be renewed or closed.
- Open exceptions are reviewed with the monthly metrics.

36. Communications and Notification Matrix

This matrix is illustrative and describes no real notification.

Event (illustrative)	Audience (illustrative)	Channel (illustrative)	Timing (illustrative)
Security incident	Affected customers	Email and portal	Within approved window
Service outage	All customers	Status page and email	On detection
Planned maintenance	All customers	Advance notice	5 business days
Vulnerability disclosure	Researchers	Security contact	Per policy
Privacy request	Requestor	Portal	Within window

Appendix D. Acronyms and Abbreviations

Acronym (illustrative)	Meaning (illustrative)
TSC	Trust Services Criteria (general framework reference)
AICPA	American Institute of Certified Public Accountants (framework body)
RTO	Recovery time objective
RPO	Recovery point objective
MFA	Multi-factor authentication
SDLC	Software development life cycle
BC	Business continuity
DR	Disaster recovery
IR	Incident response
VM	Vulnerability management
LM	Logging and monitoring
DH	Data handling
VMG	Vendor management
AC	Access control
CH	Change management
EC	Entity-level controls

37. Control Environment Narrative

This narrative is illustrative and describes no real organization or people.

37.1 Tone at the top

The executive sponsor (illustrative) sets the expectation that security and confidentiality controls are operating requirements, not optional additions. The control owners meet the executive sponsor at least annually to review the risk summary and the state of the control environment.

37.2 Commitment to competence

Personnel in control-owning roles are expected to hold or work toward relevant competence, and role-specific training is assigned annually. Competence is confirmed through the training and awareness program rather than any external credential.

37.3 Ethics and values

The acceptable-use and information-security policies (illustrative) state that personnel act with integrity, protect customer data, and report issues without fear of retaliation. This workbook itself is a demonstration artifact and makes no assertion about any real entity.

37.4 Organizational structure and authority

Control ownership is assigned by role, and each owner has a named alternate. Authority to accept risk or approve exceptions sits with the executive sponsor, and authority to approve production change sits with the platform lead.

37.5 Assignment of authority and responsibility

Responsibilities in Sections 26 and 30 trace each control area to an owner and a cadence, so no control area lacks a named accountable role.

38. Detailed Control Domain Narratives

Each narrative below describes how an illustrative control area operates. Nothing here describes a real system, person, or event.

38.1 Access control

Access is granted by least privilege using named roles, and every human account must enroll a second factor before first use. Privileged access is limited to a small set of accounts and requires additional approval. Access is reviewed quarterly: each account is confirmed to still need its role, stale accounts are revoked, and exceptions are documented with an owner and an expiry. Offboarding is triggered from the identity source and revokes access the same business day. Shared or generic accounts are not used for human work.

38.2 Change management

Production changes follow a documented lifecycle. Standard changes require a request, peer review, and an approval by a person other than the requester. A rollback plan is recorded for each change. Emergency changes may proceed to restore service but receive post-hoc review within 24 hours. Changes are tested in a staging environment that uses synthetic data only, and code is built through a continuous-integration pipeline with automated checks before deployment.

38.3 Vulnerability management

The platform is scanned on a regular cadence, and findings are triaged by severity against illustrative service-level targets. Findings are recorded in a tracker with an owner and a target date. Remediation is verified with a re-scan before closure. Dependencies are reviewed against published advisories, and vulnerable versions are pinned or upgraded. The tracker is reviewed monthly as part of the metrics program.

38.4 Logging and monitoring

Security and operational events are collected centrally and retained for an illustrative 12-month window. High-value logs are held in a write-once store so modification attempts are evident. Alerts are defined for events such as excessive failed logins, privilege changes, and unusual egress, and alert thresholds are tuned through a documented review. Logs are protected by least-privilege access and are retrievable for investigation.

38.5 Incident response

Incidents are classified by severity using a documented scheme. Detection triggers an incident log entry, assignment of an owner, and escalation by severity. Containment and eradication steps are recorded, and notification is drafted and approved before dispatch within the illustrative window. After closure, a post-incident review records lessons and opens findings in the remediation tracker. Drills and tabletops exercise the plan annually.

38.6 Business continuity and disaster recovery

Backups are taken on a regular cadence and stored encrypted. Recovery time and recovery point objectives are documented as illustrative values. Failover between zones is exercised through tabletops and a periodic restore test that verifies sample data restores within the recovery objective.

The continuity plan identifies critical services, recovery steps, and communication responsibilities, and it is reviewed after each test or material change.

38.7 Vendor management

Third parties and subprocessors are reviewed against a due-diligence checklist before engagement. The register records the service, the data involved, and the most recent review date. Vendors are re-reviewed at least annually and on material change, and offboarding removes access and confirms data disposition. The register is reviewed with the monthly metrics.

38.8 Data handling

Data is classified as customer, internal, or public, and handling rules follow the classification. Customer data is encrypted in transit and at rest, and access is least privilege and logged. Retention and deletion follow the data lifecycle table, and deletion requests are completed and verified. Non-production environments use synthetic data only.

39. Additional Evidence Samples (Part 2)

Six further filled evidence templates. All values are illustrative and synthetic.

39.1 Sample S-13: Privileged access review (filled)

Field	Value (illustrative)
Review date	2026-06-28 (illustrative)
Privileged accounts	9 (illustrative)
Confirmed needed	8 (illustrative)
Revoked	1 (illustrative)
Approver	Executive sponsor (illustrative)

39.2 Sample S-14: Alert response record (filled)

Field	Value (illustrative)
Alert	Excessive failed logins (illustrative)
Time	2026-05-19 (illustrative)
Action	Investigated and confirmed synthetic (illustrative)
Closed by	Security lead (illustrative)

39.3 Sample S-15: Capacity review (filled)

Field	Value (illustrative)
Review date	2026-06-05 (illustrative)
Peak utilization	Below threshold (illustrative)
Action	None (illustrative)
Next review	2026-07-05 (illustrative)

39.4 Sample S-16: Training completion record (filled)

Field	Value (illustrative)
Session	Data handling (illustrative)
Date	2026-03-10 (illustrative)
Completion	100% (illustrative)
Verified by	Compliance lead (illustrative)

39.5 Sample S-17: Vendor re-review record (filled)

Field	Value (illustrative)
Vendor	SP-03 messaging provider (illustrative)
Review date	2026-03-05 (illustrative)
Result	No material change (illustrative)
Next review	2027-03-05 (illustrative)

39.6 Sample S-18: Exception record (filled)

Field	Value (illustrative)
Exception	EX-01 access review (illustrative)
Approver	Executive sponsor (illustrative)
Expiry	30 days (illustrative)
Status	Open (illustrative)

40. Additional Tabletop Scenarios (Part 2)

Two further scenarios with expanded narrative. All content is illustrative.

40.1 IR-05: Synthetic phishing report from personnel

Objective: exercise the intake of an internal report of a suspicious message and the decision path for response.

Narrative (illustrative): a team member reports a suspicious message. The security lead records the report, determines the message was not delivered to other accounts, and confirms no credential entry occurred. The outcome is documented and no notification is required.

Time (illustrative)	Action (illustrative)
T+0	Report received and logged
T+10	Scope of exposure assessed
T+20	No exposure confirmed; record closed

40.2 BC-05: Synthetic backup media failure

Objective: exercise restore when a backup set is unavailable.

Narrative (illustrative): a scheduled restore test finds a backup set unreadable. The platform lead confirms a second, earlier set is intact, restores from it, and verifies integrity. A finding is opened to review backup verification.

Time (illustrative)	Action (illustrative)
T+0	Unreadable backup set detected
T+15	Earlier set located and restore started
T+45	Restore verified; finding opened

41. Additional Vendor and Vulnerability Case Files (Part 2)

Four further case files. All content is illustrative and synthetic.

41.1 VR-07: Inconsistent ownership history

Field	Value (illustrative)
Vendor	V-107 (illustrative)
Signal	Frequent ownership changes with little public record
Category	Entity stability
Disposition	Continuity and ownership requested

41.2 VR-08: Minimal public footprint

Field	Value (illustrative)
Vendor	V-108 (illustrative)
Signal	Almost no verifiable public presence
Category	Facade / opacity
Disposition	Referred for deeper check

41.3 VU-07: Weak default configuration

Field	Value (illustrative)
Finding	Service running a default configuration (illustrative)
Severity	Medium
Discovered	2026-06-15 (illustrative)
Remediated	2026-06-18 (illustrative)
Verification	Baseline applied (illustrative)

41.4 VU-08: Expired certificate on a legacy host

Field	Value (illustrative)
Finding	Expired certificate (illustrative)
Severity	Low
Discovered	2026-06-20 (illustrative)
Remediated	2026-06-20 (illustrative)
Verification	Rotated and confirmed (illustrative)

42. Control Walkthrough Narratives

Walkthroughs describe, in narrative form, how a sample transaction flows through a control. All content is illustrative.

42.1 Walkthrough: user offboarding

A departure is recorded in the identity source, which triggers revocation of the account the same business day. A reviewer confirms the account no longer appears in the access listing at the next quarterly review. The onboarding checklist is referenced for the inverse flow, so provisioning and revocation mirror each other.

42.2 Walkthrough: a standard production change

A platform engineer files a change request describing the change, the risk, and the rollback plan. A peer reviews it, and the platform lead approves it as a person other than the requester. The change is applied in staging with synthetic data, verified, then promoted. The ticket records the approval, the test result, and the implementer.

42.3 Walkthrough: a vulnerability from discovery to closure

A scan identifies a finding, which is triaged by severity and assigned an owner and target date. The owner remediates and records the change. A re-scan verifies the finding is resolved, and the tracker is updated to closed with the verification note. The monthly metrics review confirms the closure fell within target.

42.4 Walkthrough: a backup restore

A scheduled test selects a sample backup, restores it to a sandbox, and verifies integrity against expected values. The test records the restore time against the illustrative recovery objective. Any gap opens a finding in the remediation tracker.

Closing Statement

This workbook is a fictional, non-production sample prepared for demonstration only. It is not a SOC 2 report, certification, or independent attestation, and it contains no auditor opinion, seal, firm branding, badge, real address, real customer, or real person. Paper Tiger Technologies and PaperTiger are fictional.

**SAMPLE — FICTIONAL — NON-PRODUCTION — NOT A SOC 2 REPORT, CERTIFICATION, OR
INDEPENDENT ATTESTATION**