SAMPLE PREVIEW · TAILORED EVIDENCE SETUP

Compliance
Claw
ISO 27001 | evidence packs | VDR governance

ComplianceClaw Sample Tailored Evidence Pack

This is a realistic preview of the €299 Tailored Evidence Setup. ExampleCo is fictional, but the tailoring depth, document structure, and operational guidance match the intended live offer.

SAMPLE · ExampleCo | 15-person SaaS team | AWS · GitHub · Datadog | Enterprise customer review

What this preview includes

- The full Quick Wins document
- The full tailored folder structure
- The full evidence-room ReadMe
- The full scope and boundary note
- The full "Beyond This Pack" guide
- Representative checklist rows with "where to get it" + "what to save" guidance
- Representative owner-assignment rows with first-week tasks
- A realistic 4-week plan (not just a summary)

If a buyer purchases the live offer, the full checklist, complete owner map, and fully tailored planning detail are delivered against their own intake answers.

SAMPLE · EXAMPLECO

ExampleCo profile

Company: ExampleCo
Description: SaaS platform for managing employee onboarding workflows.
Team: 15 people · CEO/Founder, CTO, 6 developers, 1 DevOps, 1 HR, 2 customer support, 2 sales, 1 product
Country: Ireland
Stack: AWS · GitHub, Linear, Slack, BambooHR, Stripe, Datadog
Data handled: Customer personal data and employee personal data
Why now: An enterprise prospect asked for proof that ExampleCo can organise security evidence quickly.
Current state: The team has read about ISO 27001 but has not started in a structured way.
Existing docs: Basic acceptable use policy
Timeline: Within 3 months
Hardest part: They do not know what good evidence actually looks like in practice.
Delivery preference: Google Drive

What the sample is showing

This preview is intentionally concrete. It shows the kind of named folders, example evidence requests, ownership logic, and first-week actions a buyer would receive after completing the async intake.

SAMPLE · EXAMPLECO

00 — Quick Wins — Start Here

Quick Wins, Start Here

For ExampleCo

You do not need to read the whole pack first. Start with these. Each one should create visible progress on day one.

Win 1, Turn on proof for AWS logging

- What to do: Open AWS CloudTrail, confirm trails are enabled for management events, and save a screenshot plus the trail settings export.
- Where to save it: `A.12 Operations Security/cloud-audit-logs/aws-cloudtrail/`
- Time estimate: 5 minutes
- Why this matters: This is one of the fastest ways to show that platform activity is logged and reviewable.

Win 2, Capture root-account MFA evidence

- What to do: Check MFA on the AWS root account and primary admin users, then save screenshots showing MFA is enabled.
- Where to save it: `A.9 Access Control/mfa-evidence/`
- Time estimate: 5 minutes
- Why this matters: Prospects asking about security reviews often care about MFA before they care about deeper policy wording.

Win 3, Start the customer-review evidence thread

- What to do: Create a short internal note that names the enterprise prospect, what they asked for, and the target date for sharing first evidence-room progress.
- Where to save it: `A.18 Compliance/customer-security-review-comms/`
- Time estimate: 10 minutes
- Why this matters: It keeps the work tied to the commercial driver instead of becoming an abstract compliance project.

Win 4, Gather the current acceptable-use policy

- What to do: Save the existing acceptable use policy into the room and label it as the current version for review, not rewrite.
- Where to save it: `A.5 Information Security Policies/current-version/`
- Time estimate: 5 minutes

- Why this matters: ExampleCo already has one usable asset. Starting there creates momentum.

Win 5, Name the first evidence owners

- What to do: Fill in the named owner column for access reviews, logging, supplier management, incident response, and compliance obligations.
- Where to save it: `04-ExampleCo-owner-assignment-map-sample.csv`
- Time estimate: 10 minutes
- Why this matters: A 15-person team stalls when work is unowned. This removes that excuse immediately.

When these are done, move to `05-ExampleCo-next-step-plan.md` for the next 4 weeks.

SAMPLE · EXAMPLECO

01 — Tailored folder structure

Shown in full because the visible room structure is one of the most persuasive parts of the €299 deliverable.

```
ExampleCo ISO 27001 Evidence Room/
├── A.5 Information Security Policies/
│   ├── information-security-policy/
│   ├── acceptable-use-policy/
│   └── current-version/
├── A.6 Organisation of Information Security/
│   ├── roles-and-responsibilities/
│   ├── contact-with-authorities/
│   └── mobile-device-policy/
├── A.7 Human Resource Security/
│   ├── screening-records/
│   ├── security-awareness-training/
│   └── termination-process/
├── A.8 Asset Management/
│   ├── asset-inventory/
│   └── data-classification/
├── A.9 Access Control/
│   ├── access-control-policy/
│   ├── user-access-reviews/
│   ├── mfa-evidence/
│   ├── privileged-access/
│   └── aws-iam/
├── A.10 Cryptography/
│   ├── encryption-policy/
│   └── key-management/
├── A.11 Physical and Environmental Security/
│   └── cloud-only-note/
├── A.12 Operations Security/
│   ├── change-management/
│   ├── backup-evidence/
│   ├── logging-and-monitoring/
│   ├── datadog-alerts/
│   └── cloud-audit-logs/
├── A.13 Communications Security/
│   ├── network-security/
│   └── information-transfer/
├── A.14 System Acquisition Development and Maintenance/
│   ├── secure-development-policy/
│   ├── code-review-evidence/
│   ├── github-audit-log/
│   └── test-data-protection/
├── A.15 Supplier Relationships/
│   ├── supplier-register/
│   └── supplier-assessments/
├── A.16 Information Security Incident Management/
│   ├── incident-response-plan/
│   ├── incident-log/
│   └── lessons-learned/
├── A.17 Business Continuity/
│   ├── business-continuity-plan/
│   └── disaster-recovery-test-evidence/
├── A.18 Compliance/
│   ├── legal-register/
│   ├── privacy-policy/
│   ├── gdpr-records/
│   └── customer-security-review-comms/
```

```
└── Management Review/
    ├── risk-assessments/
    ├── management-review-minutes/
    └── internal-audit/
```

SAMPLE · EXAMPLECO

02 — Representative evidence checklist rows

The live deliverable would contain the full checklist across all relevant Annex A domains. This preview shows representative rows covering policy, access, operations, development, suppliers, incidents, continuity, and compliance.

Annex A	Control	Evidence required	Where to get it	What to save	Where to store	Priority	Owner
A.5.1	Information security policy	Approved policy PDF or tracked draft	Existing policies/docs; current acceptable-use policy as anchor	PDF export + 5-line delta note	A.5 Information Security Policies/information-security-policy/	High	Founder + CTO
A.5.10	Acceptable use rules	Acceptable use policy + acknowledgement path	Existing acceptable-use doc; onboarding checklist	Current version PDF + screenshot of acknowledgement step	A.5 Information Security Policies/acceptable-use-policy/	Medium	HR
A.6.1	Security roles and responsibilities	Named ownership + escalation path	Team roles list; Slack channel; incident contact note	1-page roles note + owner map export	A.6 Organisation of Information Security/roles-and-responsibilities/	High	CTO
A.7.2	Security awareness	Awareness proof (lightweight but real)	BambooHR onboarding; internal wiki	Screenshot/export showing onboarding includes security acknowledgement	A.7 Human Resource Security/security-awareness-training/	Medium	HR
A.8.2	Data classification	Simple classification note/matrix	Product docs; GDPR notes; data flow understanding	One-page matrix PDF	A.8 Asset Management/data-classification/	High	Product/Ops
A.9.2	Access reviews	Access review export/screenshot for key systems	AWS IAM; GitHub org; BambooHR	Export user list + note of who reviewed and date	A.9 Access Control/user-access-reviews/	High	CTO
A.9.4	MFA enforcement	Proof MFA enabled for admins/sensitive systems	AWS root/admin; GitHub org settings	Screenshots of MFA settings + org policy	A.9 Access Control/mfa-evidence/	High	CTO
A.9.5	Privileged access control	List privileged accounts + review trail	AWS admin roles; emergency access accounts	Table of admin roles + screenshot/export	A.9 Access Control/privileged-access/	High	CTO
A.12.4	Logging and monitoring	Logging/monitoring posture evidence	Datadog; CloudTrail; key service logs	Screenshot of alert rules + one representative log export	A.12 Operations Security/logging-and-monitoring/	High	DevOps
A.12.6	Backup evidence	Backup configuration + retention proof	AWS backup settings; database backups	Screenshots + short restore assumption note	A.12 Operations Security/backup-evidence/	Medium	DevOps
A.12.1	Change management	Change approval/release history evidence	GitHub PRs; Linear tickets	Screenshots/export of PR review + linked tickets	A.12 Operations Security/change-management/	High	CTO

A.14.2	Secure development	PR review + branch protection evidence	GitHub org + repo settings	Branch protection screenshot + example reviewed PR link	A.14 System Acquisition Development and Maintenance/code-review-evidence/	High	CTO
A.14.3	Test-data protection	Non-prod data handling note	Dev practices; staging setup	1-page note: do we copy prod data? if yes, controls	A.14 System Acquisition Development and Maintenance/test-data-protection/	Medium	CTO
A.15.1	Supplier management	Supplier register with risk note	Invoices; SSO app list; team knowledge	Supplier register v1 (top 10 critical vendors)	A.15 Supplier Relationships/supplier-register/	High	Ops
A.16.1	Incident response	Incident plan + incident log location	Internal wiki; ticketing tool	1-page plan + empty incident log template	A.16 Information Security Incident Management/incident-response-plan/	Medium	CTO
A.17.1	Business continuity	Backup/recovery evidence and assumptions	AWS recovery posture; runbook notes	Short restore assumption note + one backup proof artifact	A.17 Business Continuity/disaster-recovery-test-evidence/	Medium	DevOps
A.18.1	Compliance obligations	Obligations register (GDPR/contracts)	Ireland + GDPR; customer contract asks	Top 5 obligations list + quarterly review owner	A.18 Compliance/legal-register/	High	Founder

SAMPLE · EXAMPLECO

03 — Evidence room index and ReadMe

ExampleCo ISO 27001 Evidence Room, Index and ReadMe

What this room is for

This room is the working home for ExampleCo's ISO 27001 evidence. It was prepared for a live enterprise customer review and is designed to help a 15-person SaaS team collect, store, and review evidence without guessing where things belong.

How this room is organised

- Each top-level folder maps to an Annex A area or management-review function.
- Each sub-folder is named for a specific evidence type.
- Save real exports, screenshots, PDFs, and working notes into the closest matching folder before inventing new structures.
- If something is not yet polished enough to share externally, keep it in the room anyway and log the gap in the checklist notes.

How to name files

Use `YYYY-MM-DD_short-description`. Examples: - `2026-05-01_aws-cloudtrail-enabled.png` - `2026-05-03_github-branch-protection.pdf` - `2026-05-05_supplier-register-v1.xlsx`

Who should use this first

- Information security lead: CTO
- Main technical owner: DevOps + CTO
- Main operations owner: Founder / Product-Ops

Current room status

- Room created: 2026-04-28
- Primary platform: Google Drive
- Approximate evidence items in the full checklist: 60+ in the first operating pass
- Target readiness date: within 3 months

Review rhythm

- Suggested review cadence: monthly for access, logging, supplier, and incident items; quarterly for broader policy and compliance review
- Next review due: 2026-05-28

Working rule

Good enough evidence that is findable beats perfect evidence that lives in someone's inbox.

SAMPLE · EXAMPLECO

04 — Representative owner assignment rows

The live version would map the whole evidence set. This preview shows representative rows so buyers can see how responsibilities are made explicit.

Evidence area	Annex domain	Accountable	Responsible	Backup	Frequency	First 30 min	First week	Notes
Policy set	A.5	Founder	Founder	CTO	Quarterly	Find current policies and export PDFs	Mark review-existing vs create-new in the checklist	Keep scope tied to the onboarding SaaS product
Security roles and governance	A.6	CTO	CTO	Founder	Quarterly	Name security lead + escalation path	Store the owner map export and comms channel note	One named owner beats a committee
People and onboarding evidence	A.7	HR	HR	Founder	Quarterly	Locate onboarding security acknowledgement	Capture screenshot/export proving onboarding includes security	Keep proof lightweight but real
Asset and data inventory	A.8	Product/Ops	Product/Ops	CTO	Monthly	Draft 1-page data classification note	Save matrix PDF and list top assets/systems	Separate customer vs employee data clearly
Access reviews	A.9	CTO	DevOps	CTO	Monthly	Export AWS IAM + GitHub user lists	Run first access review and record date/outcome	High-signal customer-review evidence
Operations security	A.12	DevOps	DevOps	CTO	Monthly	Capture CloudTrail + Datadog proof	Save backup configuration evidence and a restore assumption note	Keep first pass grounded in current reality
Supplier management	A.15	Ops	Ops	Finance	Quarterly	Start supplier register with top vendors	Add owner + renewal month + risk note for each	Most audits stall here because it is “nobody's job”
Incident response	A.16	CTO	CTO	Founder	Quarterly	Create incident log location	Write 1-page incident response note and store it	Do not overbuild yet
Compliance obligations	A.18	Founder	Founder	CTO	Quarterly	List top 5 obligations (GDPR/contracts/customer asks)	Set a quarterly review cadence and owner	Tie obligations back to commercial pressure

SAMPLE · EXAMPLECO

05 — Next-step plan

ExampleCo, your next 4 weeks

This plan is tailored to ExampleCo's intake: AWS hosting, GitHub + Datadog, and an enterprise customer review with a 3-month target.

The goal of the next 4 weeks

By the end of Week 4, the evidence room should be usable by a reviewer without hand-holding: key exports/screenshots exist, ownership is named, and the checklist has real statuses and notes.

Week 1 (make the room real)

- [ ] Create the Google Drive root structure and top-level folders exactly as provided.
- [ ] Fill in the owner map for access reviews, logging/monitoring, supplier register, incident response, and compliance obligations.
- [ ] Complete the 5 Quick Wins and save the proof into the named folders (not just notes).
- [ ] Do a first access review for AWS IAM and GitHub: export user lists and record the review date + outcome.
- [ ] Capture CloudTrail enabled proof and one Datadog screenshot showing alert coverage.
- [ ] Create supplier register v1 with AWS, GitHub, Datadog, BambooHR, Stripe, Slack. Add owner + renewal month for each.

Week 2 (highest-signal evidence first)

- [ ] Complete the top checklist rows in order: access/MFA → logging → suppliers → incident response → compliance register.
- [ ] For each completed row, save at least one hard artifact plus a 2–3 sentence note (what it is, when captured, what's missing).
- [ ] Create a simple incident log location and store the 1-page incident response note.

Week 3 (reviewer-friendly pass)

- [ ] Do a 30-minute hygiene pass: fix naming, merge duplicates, and move misplaced files into the right annex folders.
- [ ] Add short ReadMe notes to any folder where context matters (what goes here, what "good" looks like, review cadence).
- [ ] Re-check the top 10 rows: each should have owner, status, artifact, and note.

Week 4 (operating rhythm)

- [ ] Run a checklist review session: mark what is good enough for first review vs what needs strengthening.
- [ ] Set a maintenance cadence: monthly access/logging/suppliers, quarterly policies/compliance/management review.
- [ ] Prepare a 1-page progress summary for the waiting enterprise prospect (what exists now, what’s next, target dates).

SAMPLE · EXAMPLECO

06 — Scope and boundary note

Scope and Boundary Note

For ExampleCo

This document exists so ExampleCo knows what it is getting, and what it is not. It keeps the work crisp and stops the project turning into unbounded consulting.

What this pack covers

- A tailored Google Drive folder structure for a 15-person SaaS team
- A prioritised evidence checklist shaped around an enterprise customer security review
- An owner assignment map matched to ExampleCo's current roles
- A 4-week action plan tuned for a 3-month readiness target
- Practical guidance tied to AWS, GitHub, Linear, Slack, BambooHR, Stripe, and Datadog

What this pack does not cover

- Writing every policy from scratch for you
- Legal advice
- Certification-body management
- Technical control implementation on your systems
- Unlimited or repeated multi-week revision cycles

Revision guarantee

If the deliverable does not match the stated intake use case, ComplianceClaw will revise it once at no extra charge. - Claim window: 14 days from delivery - Scope: alignment to intake and stated use case, not unlimited expansion

Regulatory and sensitivity context

ExampleCo is an Ireland-based company handling customer and employee personal data. That means GDPR-linked evidence should stay visible, current, and easy to produce during customer reviews.

If you later work with a consultant

This pack is designed to remove first-pass structure and ownership guesswork. A consultant can build on it, but ExampleCo should not wait for a consultant before collecting the first evidence.

Working rule

This pack is designed to remove guesswork, not replace every later phase of ISO 27001 work.

SAMPLE · EXAMPLECO

07 — Beyond this pack

Beyond This Pack, What Comes Next

Phase 1, evidence room setup

You are here. The room exists, the checklist is prioritised, and the immediate job is to collect evidence consistently.

Phase 2, policies and procedures

Typical next documents include: - Information security policy - Access control policy - Incident response procedure - Business continuity plan - Risk assessment methodology - Supplier review note

ExampleCo already has a basic acceptable use policy, so the right move is to review and extend it, not start from zero everywhere.

Phase 3, risk assessment

Once the room is stable, turn the biggest obvious gaps into a formal risk view. This is where ISO 27001 stops being a filing exercise and starts shaping operating decisions.

Phase 4, internal review

Before any external review, test whether the evidence is easy to find, current, and actually supports the claim being made.

Phase 5, ongoing maintenance

Keep the room alive with a simple rhythm: - Monthly: access reviews, backup checks, incident-log updates - Quarterly: management review, supplier review, risk refresh - Annually: policy review and internal audit prep

When extra help makes sense

If the room is set up but policies, risk work, or internal audit preparation feel heavier than expected, that is usually the point where ongoing monthly support becomes useful.

What a buyer does next: this sample is the proof layer. The live path is purchase → async intake → tailored pack delivery. CTA target for the website preview should point to the Tailored Evidence Setup product page and checkout flow.