SAMPLE EVIDENCE PACK

DirectiveLock

CEO Fraud Prevention

Verification Framework & Audit Evidence Pack

5	4	$2.9B	100%
Deliverable Documents	Verification Steps	Annual BEC Losses (FBI)	Audit-Ready Output

This Evidence Pack demonstrates the deliverables provided under a DirectiveLock engagement. It includes sample policy documents, approval workflows, callback scripts, sign-off logs and simulation reports. All content is structured for audit use and can be presented to auditors, insurers, or internal compliance teams as proof of process control.

Contents

01. Executive Summary

This Evidence Pack has been prepared following a DirectiveLock engagement for the purposes of internal audit, insurance review, and compliance documentation.

Organisation
ACME Global Ltd.
Finance / Operations
Engagement: April 2026

Package
Professional Implementation
5 deliverable documents
Simulation included

Status
Implementation complete
Team trained
Evidence pack sealed

Purpose of this Document

This pack serves as a structured record of the verification controls implemented under the DirectiveLock framework. It demonstrates that the organisation has adopted documented processes for approving high-risk payment requests, verifying vendor bank-detail changes, and maintaining an audit trail for each decision.

Scope of Engagement

- **Payment Approval Workflow -** Structured threshold-based approval for all payment requests above $5,000.
- **Vendor Change Lock -** Two-step verification required before any supplier bank details are updated.
- **Callback Verification -** Out-of-band phone callback to a pre-registered number for high-risk requests.
- **Role-Based Training -** Finance and management teams trained on approved channels and escalation.
- **Incident Simulation -** A controlled CEO fraud scenario run prior to live deployment.

Key Outcomes

HIGH-RISK REQUESTS
100% captured and logged through the approved request channel.

CALLBACK COMPLIANCE
Verified for all requests above the $10,000 threshold during simulation.

TEAM READINESS
All finance and operations staff completed training before go-live.

AUDIT COVERAGE
Every approved request has a timestamped sign-off log attached.

02. BEC Threat Landscape

Business Email Compromise (BEC) - also known as CEO fraud - is the highest-value cybercrime category tracked by the FBI Internet Crime Complaint Center. Unlike ransomware or data breaches, BEC exploits human behaviour rather than technical vulnerabilities. Attackers impersonate executives, vendors, or legal representatives to manipulate finance and operations staff into transferring funds or changing supplier payment details.

$2.9B	21,489	62%	3 days
Reported losses in 2023 (FBI IC3)	Complaints filed in 2023	Of attacks use impersonation only	Avg time before fraud detected

Common Attack Vectors

Executive Impersonation

Attacker spoofs a CEO or CFO email requesting an urgent wire transfer. Often timed to a Friday afternoon or during a known executive travel period.

Vendor Compromise

A legitimate supplier email account is hacked. The attacker requests a bank account change before the next invoice cycle, redirecting payments.

Invoice Fraud

A fraudulent invoice is submitted appearing to come from a known vendor, often with subtle differences in IBAN or account name.

Lawyer / Legal Impersonation

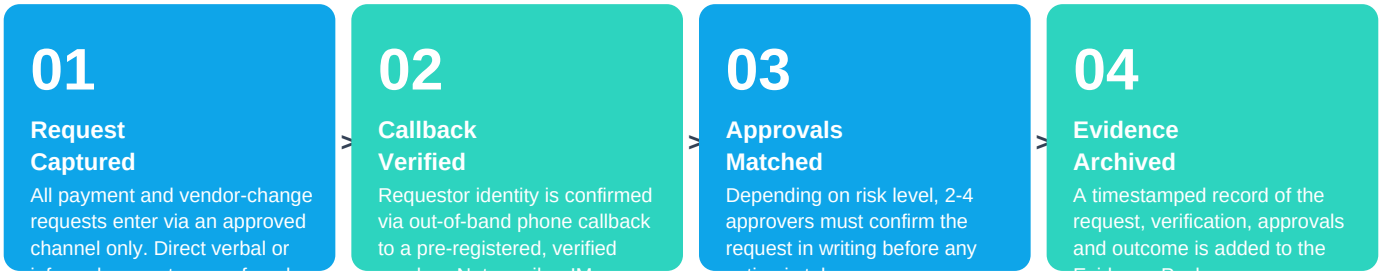
Attacker poses as external legal counsel dealing with a confidential acquisition, creating urgency and secrecy to bypass normal approval channels.

Deepfake Voice & Video

Emerging vector: AI-generated voice clones of executives used in phone or video calls to authorise transactions verbally.

03. The DirectiveLock Framework

DirectiveLock is a process-control and documentation framework, not a software product. It works by introducing friction at the exact points where BEC attacks succeed: the moment a payment is authorised or vendor details are changed. Every high-risk action must pass through four documented controls before it can be executed.



Why Process Controls Work Where Technology Fails

Email filtering, SPF/DKIM, and anti-phishing tools are necessary but insufficient. BEC attacks increasingly originate from legitimate, compromised accounts - bypassing all technical controls. A deepfake voice call bypasses every email-based defence. DirectiveLock's controls are independent of the attack channel: they require out-of-band verification regardless of how the request arrived.

Control Type	Email Filtering	MFA / SSO	DirectiveLock
Compromised account	X Bypassed	X Bypassed	**OK Out-of-band check**
Deepfake voice call	X Not applicable	X Not applicable	**OK Callback to fixed number**
Insider pressure	X Not applicable	X Not applicable	**OK Multi-approver required**
Audit evidence	Partial	Partial	**OK Full timestamped record**
Vendor bank change	X Not covered	X Not covered	**OK Dedicated lock protocol**

04. Approved Channels Policy

POLICY DOCUMENT VERSION 1.0 APPROVED

This policy defines the only channels through which high-risk payment and vendor-change requests may be initiated, communicated, and approved within the organisation.

1. Policy Statement

No payment instruction or vendor bank-detail change shall be acted upon unless it is received through an approved channel AND accompanied by a verified callback confirmation AND has obtained the required number of written approvals as defined in the Approval Matrix.

2. Approved Request Channels

PRIMARY	Designated finance request portal or shared mailbox (finance-requests@company.com)
SECONDARY	Encrypted internal messaging channel (pre-approved tool only)
ESCALATION	Direct verbal request to Finance Director, followed by written confirmation within 1 hour
PROHIBITED	Direct email from any personal or unverified account
PROHIBITED	Verbal request only (no written follow-up)
PROHIBITED	Request via personal messaging apps (WhatsApp, Signal, SMS)
PROHIBITED	Request marked as urgent with instruction to bypass normal approval

3. Mandatory Verification Steps

Step 1 - Capture
Request received via approved channel. Ticket or log entry created with timestamp, requestor name, amount/change details.

Step 2 - Callback
Finance officer initiates out-of-band callback to the requestor pre-registered phone. Call outcome logged.

Step 3 - Approval
Required number of approvers (per Approval Matrix) confirm in writing. No action until quorum is reached.

Step 4 - Archive
Complete record (request + callback outcome + approvals + action taken) added to Evidence Pack.

05. Payment Approval Workflow

WORKFLOW DOCUMENT

This workflow applies to all outgoing payment requests. Thresholds and approval requirements are defined based on transaction value and risk profile. All steps are mandatory.

Transaction Value	Risk Level	Callback	Approvers Required	Max Turnaround
< $5,000	Low	Optional	1 (Finance Lead)	Same day
$5,000 - $9,999	Medium	Recommended	1 + Manager sign-off	24 hours
$10,000 - $49,999	High	Mandatory	2 of 3 approvers	48 hours
$50,000 - $99,999	High	Mandatory	3 of 4 approvers	48 hours
$100,000+	Critical	Mandatory + recorded	CFO + CEO + Legal	72 hours
Any vendor change	High	Mandatory	2 of 3 approvers	48 hrs + docs

Refusal Protocol

- Any payment request marked "urgent" or "confidential" without prior relationship context must be escalated immediately.
- No payment shall proceed if the requestor refuses or is unavailable for callback verification.
- Requests from email addresses that do not match the pre-registered vendor directory require full re-verification.
- A 24-hour hold applies to all first-time vendor payments above $5,000 regardless of approval status.

06. Vendor Change Lock Protocol

HIGH-RISK PROTOCOL

Vendor bank detail changes are among the most exploited vectors in BEC fraud. This protocol applies to any request to modify the IBAN, account name, sort code, or payment reference for an existing supplier, regardless of the communication channel.

1. **Request Received**
   Change request arrives via approved channel only. Direct email from vendor to a single finance employee does not qualify.
2. **Source Verification**
   Finance team calls the vendor using the telephone number on file - NOT the number provided in the change request.
3. **Document Collection**
   Vendor supplies: (a) signed letter on headed paper, (b) bank statement or bank confirmation letter, (c) photo ID of authorised signatory.
4. **Director Sign-Off**
   Finance Director reviews documents and approves in writing. Minimum 48-hour review period before change is activated.
5. **Change Activated**
   Account details updated in the payment system. Old details archived. Confirmation sent to pre-registered vendor email only.
6. **Test Payment**
   A EUR 1 test transfer is made to the new account. Vendor confirms receipt before any full payment is processed.
7. **Evidence Archived**
   Complete record filed: request, verification log, documents received, approvals, test payment confirmation.

07. Callback Verification Script

TRAINING SCRIPT

This script is used by the finance officer when performing an out-of-band callback verification. The call must be placed to the pre-registered telephone number on file - never to a number provided in the payment request itself.

INTRO	Hello, this is [Name] from [Company] Finance. I am calling to verify a payment request we received. Is this [Requestor Name]?
CONFIRM	Can you confirm the request details? We have received a request for [Amount] payable to [Vendor/Recipient]. Is that correct?
VERIFY	Before we can proceed, I need to ask you a few verification questions. These are mandatory for all payments above our threshold.
Q1	What is the cost centre code or purchase order reference for this payment?
Q2	Which budget holder has pre-approved this expenditure?
Q3	Is there any reason this should be treated as time-sensitive or confidential?
NOTE	If requestor asks to skip: I understand this may feel like a delay, but our policy requires this for all payments of this size. I cannot proceed without completing verification. I can escalate to our Finance Director if needed.
CLOSE	Thank you. I will process this within [standard timeframe] once approvals are confirmed. You will receive confirmation to your registered email address.

! Red Flags - End Call and Escalate Immediately

Requestor cannot answer basic questions | Requestor asks for confidentiality | Request involves a new or recently changed bank account | Requestor becomes hostile or pressures you to proceed

08. Approval Matrix

APPROVAL MATRIX ACTIVE

The following matrix defines who can approve payment and vendor-change requests at each risk level. Quorum means the required number of the listed approvers must all confirm in writing.

Risk Level	Threshold	Approver Roles	Quorum	Callback	Max Time
Low	< $5,000	Finance Lead	1 of 1	Optional	Same day
Medium	$5k-$9.9k	Finance Lead + Manager	1 of 2	Recommended	24 hours
High	$10k-$49k	Finance Lead, Manager, FD	2 of 3	Mandatory	48 hours
High	$50k-$99k	FL, Mgr, FD, CFO	3 of 4	Mandatory	48 hours
Critical	$100k+	CFO, CEO, Legal	All 3	Mandatory + recorded	72 hours
Vendor Chg	Any	FL, FD, CFO	2 of 3	Mandatory	48 hrs + docs

Approver Register

Role	Name	Email	Verified Phone	Type
Finance Lead	Jane Mitchell	j.mitchell@company.com	+44 7700 900 001	PRIMARY
Finance Director	Robert Langford	r.langford@company.com	+44 7700 900 002	PRIMARY
CFO	Sarah Chen	s.chen@company.com	+44 7700 900 003	PRIMARY
CEO	Marcus Webb	m.webb@company.com	+44 7700 900 004	ESCALATION
Legal Counsel	David Torres	d.torres@legalfirm.com	+44 7700 900 005	ESCALATION

09. Risk Classification Guide

LOW RISK
$0 - $4,999

- Single approver required.
- Callback optional but recommended for new payees.
- Standard processing time applies.
- Basic log entry required.

MEDIUM RISK
$5,000 - $9,999

- Two-step approval required.
- Callback strongly recommended.
- 24-hour processing window.
- Log entry with manager countersignature.

HIGH RISK
$10,000 - $99,999

- Mandatory out-of-band callback.
- Minimum 2 of 3 approvers required.
- 48-hour processing window.
- Full Evidence Pack entry required.
- Finance Director notification on initiation.

CRITICAL
$100,000+ / Any new ba

- Mandatory callback - recorded.
- CFO + CEO + Legal must all approve.
- 72-hour minimum processing window.
- Board notification required.
- External verification recommended for amounts above $500k.

10. Role-Based Training Checklist

FINANCE TEAM COMPLETED

To be completed by all finance and accounts payable staff before go-live date.

MODULE 1 - BEC Threat Awareness

- [x] Understands what Business Email Compromise is and how it works
- [x] Can identify the 5 most common BEC attack vectors
- [x] Knows that verified email addresses can be compromised
- [x] Understands why urgency and secrecy are red flags

MODULE 2 - Approved Channels Policy

- [x] Knows which channels are approved for payment requests
- [x] Can identify a prohibited request channel
- [x] Knows the correct action when a request arrives via wrong channel
- [x] Has read and signed the Approved Channels Policy document

MODULE 3 - Callback Verification

- [x] Can perform a callback using the registered number directory
- [x] Has memorised or bookmarked the callback verification script
- [x] Knows when callback is mandatory vs optional
- [x] Has practised at least one simulated callback scenario

MODULE 4 - Approval Workflow

- [x] Knows the payment threshold tiers and their requirements
- [x] Can identify who to contact for each approval tier
- [ ] Knows the maximum turnaround time for each tier
- [x] Has completed a practice run of the approval workflow

Role-Based Training Checklist

MANAGEMENT & DIRECTORS COMPLETED

To be completed by all directors, department heads, and designated approvers.

MODULE 5 - Executive-Level Threat Awareness

- [x] Understands deepfake voice and video threats and why they require process controls
- [x] Aware that own identity may be impersonated in fraud attempts
- [x] Has briefed direct reports on the importance of verification compliance
- [x] Knows own responsibilities under the Approved Channels Policy

MODULE 6 - Approval Responsibilities

- [x] Knows which requests require director-level sign-off
- [x] Has registered phone number in the verified approver directory
- [x] Understands that verbal-only approvals are not sufficient or valid
- [x] Has reviewed and signed the Approval Matrix document

MODULE 7 - Incident Response

- [x] Knows the first steps if a potential fraud attempt is identified
- [x] Has contact details for the designated incident escalation point
- [x] Understands that no payment reversal is guaranteed once processed
- [x] Has participated in the DirectiveLock simulation exercise

MODULE 8 - Ongoing Compliance

- [x] Committed to not bypassing verification controls even under time pressure
- [x] Understands that confidential requests do not override process requirements
- [ ] Has agreed to quarterly review of approver directory and thresholds
- [x] Aware of reporting obligation to Finance Director for any suspected attempt

Training Sign-Off

Name	Role	Date Completed	Signature

11. Incident Simulation Report

SIMULATION | SCENARIO A - CEO WIRE FRAUD | PASSED

Date	Facilitator	Participants	Duration
14 April 2026	DirectiveLock	4	2h 30m

Scenario Description

The simulation tested the response to a spoofed CEO email requesting an urgent wire transfer of $47,500 to a new overseas vendor. The email appeared to originate from the CEO legitimate address and was sent during a known period of CEO travel. The message instructed the finance officer to process the payment immediately and not to discuss it with others until confirmed.

Timeline of Events

- **09:14** Email received by Finance Officer (Jane Mitchell) - spoofed CEO address, urgent tone.
- **09:16** JM identifies request as High Risk ($47.5k) - initiates approved channel log entry.
- **09:18** JM checks vendor against approved vendor directory - vendor not found. Flag raised.
- **09:22** JM attempts callback to CEO pre-registered number - CEO confirms no such request made.
- **09:25** Finance Director (Robert Langford) notified. Request flagged as suspected fraud.
- **09:31** IT Security notified. Spoofed email headers preserved as evidence. No payment processed.
- **09:45** Full debrief conducted. Evidence Pack entry created. Process logged as correctly followed.

Simulation Scoring Rubric

Process Compliance 95/100

Finance officer followed approved channel policy without prompting.

Callback Execution 100/100

Out-of-band callback initiated within 5 minutes of receiving request.

Vendor Verification 90/100

New vendor correctly identified as unregistered before callback.

Escalation Speed 85/100

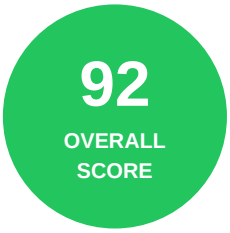
Finance Director notified within 10 minutes of fraud identification.

Evidence Capture 100/100

All steps logged with timestamps before end of working day.

Team Communication 80/100

One team member initially shared request details informally - minor breach.



Recommendations

- All-hands reminder that payment request details should not be shared informally before verification is complete.
- Add a confidentiality of requests clause to the next team training refresh (scheduled Q3 2026).
- Consider implementing a 30-minute hold on all High-risk requests to allow verification window.

12. Sample Request Log Entry

REQUEST #DL-2026-0047 VERIFIED PROCESSED

Request ID	DL-2026-0047
Date & Time	22 April 2026 - 14:32 UTC
Request Type	Payment authorisation
Requestor	Marcus Webb (CEO) - m.webb@company.com
Received Via	Approved finance request portal
Payee	Deltaflow Systems GmbH
IBAN	DE89 3704 0044 0532 0130 00
Amount	EUR 23,750.00
Reference	Invoice INV-2026-0341 - Q2 server infrastructure
Purchase Order	PO-2026-117 (pre-approved by IT Director, 18 April 2026)
Urgency Claimed	None - standard payment terms
New Payee?	No - registered vendor since March 2025

Verification Record

Callback Performed	Yes - 14:38 UTC
Number Called	+44 7700 900 004 (registered CEO mobile - verified directory)
Call Duration	3 minutes 12 seconds
Call Outcome	CEO confirmed request. Reference and amount verified verbally.
Callback Officer	Jane Mitchell (Finance Lead)
Approver 1	Robert Langford (Finance Director) - Approved 14:52 UTC
Approver 2	Sarah Chen (CFO) - Approved 15:04 UTC
Quorum Met	Yes - 2 of 3 required (High Risk threshold)
Payment Processed	22 April 2026 - 15:11 UTC
Evidence Pack Entry	Appended to DL-2026-0047.pdf - 15:14 UTC

13. Sign-Off Log

APRIL 2026 | 8 ENTRIES

Timestamped log of all verification sign-offs for the period.

Ref	Date	Type	Amount	Requestor	Approvers	Status
DL-2026-0040	03 Apr	Payment	EUR 4,200	J. Mitchell	1 of 1	Processed
DL-2026-0041	07 Apr	Vendor Chg	--	R. Langford	2 of 3	Processed
DL-2026-0042	09 Apr	Payment	EUR 14,500	M. Webb	2 of 3	Processed
DL-2026-0043	11 Apr	Payment	EUR 7,800	S. Chen	1 of 2	Processed
DL-2026-0044	14 Apr	SIMULATION	EUR 47,500	CEO (spoofed)	--	BLOCKED
DL-2026-0045	17 Apr	Payment	EUR 2,100	J. Mitchell	1 of 1	Processed
DL-2026-0046	19 Apr	Payment	EUR 88,000	M. Webb	3 of 4	Processed
DL-2026-0047	22 Apr	Payment	EUR 23,750	M. Webb	2 of 3	Processed

Log Summary

8
Total Requests

7
Processed

1
Blocked / Refused

100%
Callback Rate (High Risk+)

38 minutes
Avg Approval Time

100%
Policy Compliance

14. Evidence Pack Structure

The Evidence Pack is a structured archive of all verification activity. It is maintained in real time and can be exported at any point for audit, insurance, or compliance review.

01 - Policy Documents

- Approved Channels Policy (signed)
- Payment Approval Workflow
- Vendor Change Lock Protocol
- Approval Matrix (current version)

02 - Training Records

- Finance Team Training Checklist (signed)
- Management Training Checklist (signed)
- Training attendance register
- Simulation participation log

03 - Request Logs

- Individual request log entries (one file per request)
- Monthly sign-off log summary
- Callback verification records
- Approval confirmation emails (archived)

04 - Simulation Reports

- Simulation scenario description
- Participant response log
- Scoring rubric and outcome
- Post-simulation recommendations

05 - Incident Records

- Blocked or refused request logs
- Escalation records
- External notifications (where applicable)
- Post-incident review notes

15. 30-Day Implementation Timeline

WEEK 1
Discovery
. Risk mapping session (payment, vendor, approval flows)
. Identify high-risk roles and decision points
. Review existing controls and gaps
. Confirm approver register and phone numbers

WEEK 2
Design
. Draft Approved Channels Policy
. Build Approval Matrix to organisation thresholds
. Configure request log template
. Prepare Vendor Change Lock Protocol

WEEK 3
Deploy + Train
. Distribute and sign all policy documents
. Conduct finance team training (Module 1-4)
. Conduct management training (Module 5-8)
. Set up evidence archive structure

WEEK 4
Simulate + Protect
. Run incident simulation exercise
. Review simulation results and scoring
. Address any gaps identified
. Issue completed Evidence Pack - go-live

What You Receive at Completion

Deliverable	Description
Signed Policy Package	All policy documents countersigned by relevant stakeholders.
Populated Approval Matrix	Customised to your organisation thresholds, roles, and contacts.
Training Records	Signed checklists for all trained staff, retained for 3 years.
Simulation Report	Scored incident simulation with recommendations.
Live Evidence Archive	Ongoing request log structure, ready for audit export at any time.

16. Frequently Asked Questions

Is DirectiveLock a software product?

No. DirectiveLock is a process-control and documentation framework. There is no software to install or maintain. The deliverables are policy documents, workflow templates, training materials, and an evidence archive structure - all designed to be operated by your existing team using existing tools.

How long does implementation take?

The standard implementation runs over 30 days across four phases: Discovery, Design, Deploy & Train, and Simulate. For smaller organisations with fewer decision-makers, implementation can be compressed to 2-3 weeks.

Do we need to change our existing software or systems?

No. DirectiveLock works alongside whatever payment, communication, and document management tools you already use. The framework defines process requirements; it does not replace technology.

What if a payment request comes in urgently?

Urgency is itself a red flag in BEC fraud. The framework explicitly addresses this: no amount of urgency overrides the verification requirement. Faster processing can be arranged within the framework - but the verification steps remain mandatory.

Can this be adapted for a multi-entity organisation?

Yes. The Professional and Enterprise packages include custom approval architecture for organisations with multiple entities, currencies, or locations. Additional approver tiers and localised policies can be added during the Design phase.

Does the Evidence Pack hold up in an insurance claim?

DirectiveLock is designed with audit and insurance review in mind. The timestamped logs, signed approvals, and callback records demonstrate a structured verification process was followed. This does not constitute a legal guarantee of insurance acceptance.

What ongoing support is available after implementation?

Optional ongoing support is available from $249/month. This includes quarterly policy review, approver directory updates, staff refresher training, and access to updated simulation scenarios as fraud patterns evolve.

Legal Notice

IMPORTANT - PLEASE READ BEFORE RELYING ON THIS DOCUMENT

This document is a sample Evidence Pack produced by DirectiveLock for demonstration and evaluation purposes. All names, companies, reference numbers, amounts, and dates contained herein are fictitious and are used for illustrative purposes only. Any resemblance to real persons, organisations, or transactions is coincidental.

SCOPE OF SERVICE

DirectiveLock provides process documentation, verification workflow design, training materials, and evidence-pack structure. DirectiveLock is not a regulated financial service, cybersecurity firm, legal practice, or insurance provider. Nothing in this document constitutes legal advice, financial advice, cybersecurity certification, or insurance coverage.

NO GUARANTEE

No fraud-prevention process can guarantee that an incident will never occur. The purpose of DirectiveLock is to reduce execution risk by requiring approved channels, out-of-band verification, clear approvals, and evidence capture. Implementation of this framework does not constitute a guarantee against loss.

CONFIDENTIALITY

This Evidence Pack is prepared for the exclusive use of the named organisation. It should not be shared with third parties without authorisation, except as required for audit, legal, or insurance review purposes.

INTELLECTUAL PROPERTY

The framework structure, document templates, workflow designs, and training materials contained within this Evidence Pack are the intellectual property of DirectiveLock. They may be used internally by the licensed organisation but may not be resold, redistributed, or sublicensed without express written consent.

GOVERNING LAW

These terms are governed by the laws of the jurisdiction in which the licensed organisation is incorporated, unless otherwise agreed in writing at the time of engagement.