BCON COLLECTIVE
By Bridewell

HIRING IS AN ATTACK SURFACE

# Defending Against DPRK IT Workers – An Implementation and Operational Guide

Date: 17/08/2026

Version: 1.0

# CONTENTS

# HIRING IS AN ATTACK SURFACE

## An implementation guide and operational workbook for defending against DPRK IT workers

This guide gives security leaders and their cross-functional teams a practical route for building and operating a DPRK IT worker defence programme, from application through the first 90 days.

| 1 UNDERSTAND AND PLAN | 2 DETECT AND RESPOND | 3 OPERATE A CASE |
|---|---|---|
| Choose a maturity level and build the programme. | Run maturity-appropriate hunts and coordinate response. | Set up the stage, then open the case sheet and current-stage form. |

*One authoritative source: the writable forms, scoring guardrails and signal definitions are all contained in Part 3.*

**There is a question worth asking about your last remote technical hire.**

Was the person who submitted the application the same person who attended the first interview? Was that person the same one who appeared in the next round? And are either of them the person currently holding your production credentials?

For most hires, the answer is yes. In a Democratic People's Republic of Korea (DPRK) information technology (IT) worker operation, it may not be.

DPRK IT workers represent a **state-directed insider threat capability** that combines revenue generation with trusted access into foreign organisations. Using fabricated, stolen identities or rented identities, North Korean personnel obtain legitimate employment as remote developers, engineers and contractors, placing DPRK-linked actors inside trusted corporate environments rather than requiring them to breach those environments from the outside. Their principal mission remains generating foreign currency for the regime, but the access they acquire can also create opportunities for credential theft, intellectual property collection, data theft and other malicious activity.

The IT worker programme should therefore be understood as part of the DPRK's wider cyber and revenue-generation ecosystem, not simply a standalone employment-fraud scheme. Government and industry reporting shows overlap between IT-worker activity and the DPRK's broader cyber apparatus, including links through state organisations, facilitators, infrastructure and operational objectives. IT workers also provide something conventional intrusion teams cannot easily replicate: legitimate identities, established business relationships and trusted access inside victim organisations. That access can support both financial objectives and wider malicious activity.

The identity may be stolen, rented or fabricated. An interview specialist may pass the assessment. A domestic facilitator may receive the corporate laptop. An overseas operator may then control the device through remote-access software or hardware. Several people may rotate behind one employee identity.

This changes the security problem. The organisation is not dealing with an external attacker trying to steal credentials. It is using a legitimate business process to create the account, issue the device and grant the access.

**The problem is simple:** no single team can see the whole DPRK IT worker operation. Recruitment sees the applicant, HR sees the identity, IT and IAM see the device and account, the SOC sees post-hire activity, Procurement sees the supplier, and Finance sees the payment. Each part may look legitimate on its own, which allows breaks in identity and access continuity to go unnoticed.

**A joined cross-functional view is therefore essential, not optional.** Security leadership must bring these teams together around shared evidence, common escalation points and clear decision ownership. When that happens, weak signals become more meaningful, investigations move faster, and the organisation is much better placed to identify and disrupt the operation before trusted access is abused.

HM Treasury's Office of Financial Sanctions Implementation assesses it is almost certain that UK firms are being targeted.[1] Google and Microsoft have reported European expansion, stolen identities and artificial intelligence (AI)-enhanced recruitment activity.[2][3] The Federal Bureau of Investigation (FBI) and US Department of Justice have documented data theft, extortion and domestic laptop-farm facilitators.[4][5] A multinational government alert issued on 31 July 2026 further highlighted third-party proxies, remote-access tooling, payment diversion and account behaviour consistent with coordinated operations.[13]

**BCON Collective built this framework because the problem facing security leaders is not a lack of warning signs. It is turning them into a programme that can actually be deployed and operated.** Customers have limited time, competing priorities and different levels of existing capability, and need to know what to implement first rather than trying to deploy every recommendation at once. Existing guidance contains valuable recommendations, but these are often treated as individual checks rather than signals that can be connected across the employment lifecycle. The stronger approach is to link evidence from application and interview through onboarding, device and account use, work activity, suppliers and payment, so that each stage contributes to the same view of identity and access continuity.

Developed while advising a customer on this challenge, the framework turns that fragmented guidance into a clear implementation and operational plan. It sets out what to build first, what depends on what, who owns each control, how to test it and how to bring the resulting evidence into one case. The aim is to make a difficult cross-

functional insider-threat programme practical to deploy, simple to understand and capable of adapting as DPRK IT worker tradecraft evolves.

The central conclusion was simple:

> **The applicant is not the unit of trust. Identity continuity is.**

The defensive question is not, "Can we prove this person is a DPRK operative?" It is:

> **Can we establish that the same person controls the same identity, communications, device and work product from application through employment?**

This guide provides a starting point for organisations at four levels of maturity. It applies to employees, contractors, outsourced development teams, staffing suppliers and online procurement routes, including subsidiaries where hiring and endpoint controls may be weaker. Part 3 contains the complete operational workbook, so the same controlled document can be used to design the programme and operate a case.

**Analytic note:** The complete programme has not been deployed or the scoring weights validated against a controlled population. The scores are calibration starting points, not probabilities or attribution judgements. Every escalation should remain human-led and supported by evidence from more than one source.

# PART 1 — UNDERSTAND AND PLAN

# THE OPERATION IS A PRODUCTION LINE

The most important insight is that this threat is not always one person pretending to be someone else. It can be a production line in which different people manage the application, interview, device, daily work and payment.

Every handoff creates a seam. That is why controls that test continuity across stages are more durable than controls that look for one suspicious face, accent or Internet Protocol (IP) address.

At least five attack models have been used by DPRK IT Workers.

| *ATTACK MODEL* | HOW IT WORKS | WHAT DEFEATS IT |
|---|---|---|
| **AM1: Solo operator using virtual private network (VPN) or proxy infrastructure** | One person applies, interviews and works from outside the claimed country while masking location. | Repeated identity checks, sign-in analysis, endpoint controls and working-pattern review. |
| **AM2: Operator using a domestic laptop farm** | A facilitator receives the device and enables remote control from overseas while the laptop remains on a trusted domestic network. | Verified delivery, shared-address analysis, remote monitoring and management (RMM) detection and remote-hardware visibility. |
| **AM3: Domestic facilitator or interview proxy** | A genuine local person attends interviews or onboarding and then hands access to the overseas operator. | Post-onboarding identity re-verification and detection of the handoff on the device. |
| **AM4: Assembly-line persona relay** | Different people manage applications, communications, interviews, logistics and daily work behind one identity. | Cross-stage callbacks, communication continuity, entity resolution and multi-channel checks. |
| **AM5: AI-augmented operation** | AI improves documents, photographs, translation, interviews or coding output. DPRK-linked cyber activity has also demonstrated local LLM, RAG, speech-to-text and agentic experimentation in actor-controlled infrastructure; these capabilities may transfer to IT-worker operations, but this is not evidence of current programme-wide use.[16] | Physical and channel continuity, device/account binding, mission-behaviour detection and corroborated scoring. Do not score AI use itself. |

*Table 1. Five DPRK IT worker operating models and their principal defensive weaknesses*

Looking at these different models, three implications follow.

1. **Geography is not identity.** A compliant device on a domestic IP address may still be controlled from overseas.
2. **Passing an interview is not continuity.** The person who passes the assessment may not be the person who receives access.
3. **A trusted account changes detection.** Once hired, the operator's activity can resemble legitimate work unless identity, endpoint and data signals are correlated.

The continuity chain does not end with the interview. It runs across the five linked assets shown in Figure 1. An in-person meeting establishes that a real person attended; it does not establish who will control the account, perform the work or receive the funds after onboarding. The July 2026 multinational alert specifically warns that proxies may attend interviews or in-person meetings and that payments may be redirected to third-party accounts.[13]

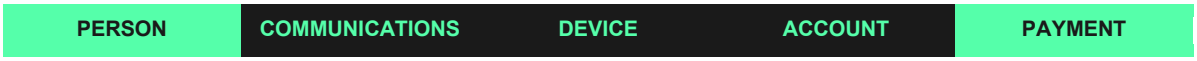


*Figure 1. The identity-continuity chain that the organisation must preserve*

*A break at any point becomes part of the same case: who applied, who controlled the channels, who possessed the device, who used the account and who received the funds.*

**Analytic note:** DPRK IT worker activity is not synonymous with malicious recruitment campaigns such as Contagious Interview. In the former, the operator seeks employment and trusted access; in the latter, the actor poses as the recruiter and compromises the candidate. Operators or infrastructure may overlap, but the objectives, evidence and defensive workflows differ.[14]

The attack models show why no single control can cover the threat. The practical question is not whether an organisation can implement every recommendation, but which controls remove its largest current gaps. The maturity model below provides that starting point.

# FIND YOUR STARTING POINT IN 60 SECONDS

This is a maturity assessment for the DPRK IT worker control problem, not a judgement on the organisation's overall security programme.

Count how many statements are true today:

☐ A named owner is accountable for the programme and in-scope roles are documented.

☐ The applicant tracking system (ATS) or Human Resources (HR) team checks for reused phone numbers, email addresses, physical addresses and near-identical curriculum vitae (CV) content.

☐ Equipment delivery is bound to a verified person and address, with redirects controlled.

☐ The SOC has tested detection for unapproved remote monitoring and management (RMM) tools and failed installation attempts on new devices.

☐ Line managers repeat a live identity check during the first weeks of employment.

☐ HR and Security can contribute to one restricted case record.

☐ A calibrated, human-led scoring model is used to select the next verification step.

☐ The organisation runs retrospective hunts and exercises the laptop-farm and proxy-handoff scenarios.

| SCORE | STARTING LEVEL | WHAT IT MEANS |
|---|---|---|
| **0-2** | **LEVEL 1: FOUNDATION** | ESTABLISH BASIC IDENTITY, DELIVERY AND ENDPOINT CONTROLS. |
| **3-4** | **LEVEL 2: DEVELOPING** | CONNECT THE TEAMS AND EXTEND ASSURANCE INTO THE FIRST 90 DAYS. |
| **5-6** | **LEVEL 3: MATURE** | ADD CROSS-STAGE TESTS, STRUCTURED SCORING AND RECURRING HUNTS. |
| **7-8** | **LEVEL 4: ADVANCED** | AUTOMATE CORRELATION, TEST REMOTE HARDWARE AND CONTINUOUSLY ADAPT THE MODEL. |

*Table 2. Rapid maturity assessment and recommended starting level*

Use Table 2 to select the level that matches your current capability, then follow Table 3 before reading the detailed level controls. Do not wait for an advanced programme before implementing the controls that remove the largest gaps.

# START HERE: SEVEN STEPS TO A WORKING PILOT

Use this sequence before treating the guide as a control catalogue. Start with one role or hiring route, prove the minimum controls work, and add scoring or advanced hunts only when their prerequisites exist.

**Do not confuse maturity levels with case tiers.** A maturity level describes what capability the organisation has built. A case tier describes how the organisation responds to evidence about one candidate or employee. A foundation organisation can still have a critical security case, but it should not deploy an advanced scoring workflow it has not trained or governed.

| STEP | ACTION | PRIMARY OWNER | DONE WHEN |
|---|---|---|---|
| 1 | Choose one pilot scope | Programme Owner + HR | One business unit, role type, contractor route or recent-hire population is approved. |
| 2 | Name owners and approve guardrails | Programme Owner | HR, SOC, Legal/Data Protection, Finance and Procurement contacts accept their roles; retention and escalation are documented. |
| 3 | Implement the minimum viable four in parallel | HR + IT + SOC + line managers | Duplicate screening, controlled delivery, remote-access detection and first-weeks re-verification each pass one acceptance test. |
| 4 | Create one restricted case process | HR + Security + Data Protection Officer | A synthetic case records fact, evidence, explanation, owner, decision and deletion date without email-only handoffs. |
| 5 | Run one tabletop or retrospective scenario | CTI + SOC + HR | A laptop-farm or proxy-handoff scenario closes with actions, evidence gaps and decision rights recorded. |
| 6 | Pilot the score with trained reviewers | Security reviewer + HR coordinator | Two reviewers agree on root cause, domains, tier and next action for one synthetic or retrospective case. |
| 7 | Add hunts and scale only where data exists | SOC + CTI + control owners | Each selected hunt has data, logic, owner, cadence and a tested benign and adversarial outcome. |

*Table 3. Seven-step adoption map: order, ownership, output and exit condition*

# IF CAPACITY ALLOWS ONLY FOUR CONTROLS

**If your capacity will only allow you to follow four controls, these are our top recommendations.**

1. Weekly duplicate checks across applicants and recent hires.
2. Equipment delivery or assigned VDI/work environment bound to the verified person and account; control redirects where physical equipment is issued.
3. Detection for unapproved remote access, secondary VPNs and failed installation attempts, active before first login.
4. A live identity re-verification during weeks two or three.

Do not begin with advanced interview traps or the full scorecard.

# OPTIONAL PILOT CADENCE

Use this only as a planning aid after Table 3. Exit evidence, not elapsed time, controls progress; an organisation may remain at foundation for the whole pilot and still succeed.

Before live activation, brief HR, recruitment, hiring managers, CTI, the SOC, insider risk, finance, procurement, legal and the DPO on evidence flow, scoring limits and decision ownership.

| *PHASE* | AIM | USE | EXIT EVIDENCE |
|---|---|---|---|
| *Before live use* | Authorise the pilot | Table 3 steps 1-2 plus the Part 3 universal prerequisites. | Scope, owners, guardrails and success measures are approved. |
| *First implementation cycle* | Prove Foundation | Build and acceptance-test the in-scope Foundation outcomes in Tables 5 and Part 3; run Hunt 1 when its data is ready. | Every in-scope Foundation row is Ready or formally Out of scope and the seeded tests pass. |
| *Next cycle* | Connect evidence | Add the Developing capabilities, shared case process and only the scoring/hunts supported by available evidence. | One synthetic or retrospective case joins HR, identity, device and administrative evidence end to end. |
| *Scale on exit evidence* | Add Mature or Advanced methods deliberately | Use Tables 7-8 as roadmaps and Part 3 as the implementation authority. | Reviewer agreement, alert quality, ownership and response remain within approved tolerances. |

*Table 4. Optional pilot cadence — progress only when exit evidence exists*

**Measure whether the programme is working, not how many people it escalates.** Useful measures include how much of the in-scope workforce is covered, whether controls work when tested, whether verified delivery and first-weeks checks are completed, the quality of the evidence being collected, how quickly the right teams can come together to review a case, and whether different reviewers reach broadly consistent decisions. You should also test the programme against realistic scenarios to make sure it can detect the behaviours it was designed to find.

**Do not use the number of candidates escalated as a measure of success.** A good programme may generate relatively few escalations because its controls are working earlier in the process and its evidence thresholds are well calibrated.

# ONLY IMPLEMENT YOUR CURRENT MATURITY LEVEL

Tables 5-8 are roadmaps, not setup instructions. Use them to select the outcomes for your current maturity, then build and acceptance-test those outcomes in Part 3. Part 3 is authoritative if wording differs.

Throughout the maturity tables, short codes point to the detailed controls and setup guidance elsewhere in the guide. Levels 1–4 describe organisational maturity, not case severity; AM1–AM5 are threat operating models; E01–E07 are reusable build-once capabilities; and ID, COM, PHY, DEV, MIS and ADM identify individual checks across identity, communications, physical identity, device/access, mission/data and administration/finance.

Hunt 1–4 refers to the SOC hunt playbooks in Part 2, while references such as Onboarding baseline or First-90-days baseline point to evidence that must already have been created at that stage. A number such as ID-03 identifies the specific check, and a weight such as (+3) is its fixed score when the stated scoring condition is met.

# LEVEL 1: FOUNDATION

**Best for:** organisations with limited insider-risk capability, decentralised recruitment or no dedicated DPRK IT worker process.

**Objective:** bind the applicant, device and account together, then detect the most common remote-control path.

**Implementation boundary. Do now: complete every Level 1 row and run Hunt 1.**

| ORDER | OUTCOME | IMPLEMENT THROUGH | PROOF |
|---|---|---|---|
| 1 | Programme governance is in scope | Universal prerequisites + implementation status dashboard | Scope, owner, decision rights and escalation route are approved. |
| 2 | Duplicate applicants and related records are detectable | E01 + Application ID-02/ID-03 | Seeded duplicate contact/address records are surfaced with an owner. |
| 3 | A retrievable live hiring baseline exists | E02 + E03 + Interview 1 baseline | A later stage can securely retrieve and compare the baseline. |
| 4 | Device or VDI is bound before access | E05 + E07 + Onboarding baseline | A redirect, reassignment or visibility gap creates a formal exception. |
| 5 | Unapproved remote access is detectable | E07 + DEV-01 + Hunt 1 | Approved support is suppressed and a seeded RMM chain creates one contextualised case. |
| 6 | The person is reverified after joining | E02 + E03 + PHY-06 | A mock week-two/week-three mismatch joins the case and reaches the review route. |
| 7 | New-starter access remains least privilege | E07 work/access baseline + First-90-days baseline | 30/60/90-day reviews complete and exceptions are approved. |

*Table 5. Foundation outcomes and authoritative implementation path*

For contractor-heavy organisations, prioritise duplicate screening, controlled delivery, RMM detection and the week-two check. These controls address the facilitator-proxy model that most pre-hire checks miss.

**When am I ready to progress?**

You are ready to progress when HR, IT and the SOC can show that every in-scope hire has gone through the same baseline controls, and that those controls have been tested in practice rather than simply documented.

# LEVEL 2: DEVELOPING

**Best for:** organisations with established endpoint and identity tooling but weak coordination between recruitment and security.

**Objective:** make evidence survive the handoffs between HR, interviewers, onboarding, finance and the SOC.

**Implementation boundary. Do now: build the shared case process, pilot the score on synthetic or retrospective evidence, and run Hunts 1 and 4.**

| ORDER | OUTCOME | IMPLEMENT THROUGH | PROOF |
|---|---|---|---|
| 1 | HR and Security share one governed case | Universal prerequisites + case sheet | Both teams can contribute with tested access, audit and retention controls. |
| 2 | Identity and references are independently verified | E02 + ID-04/ID-05 + PHY-05 | Evidence is independently sourced, bound to the live baseline and unresolved mismatch routes correctly. |
| 3 | First-90-day security context is joined | E07 + Onboarding/First-90-days baselines | A seeded first-login event reaches the right owner with user/account/device-or-VDI context. |
| 4 | Administrative changes preserve continuity | E04 + E06 + ADM-01/ADM-02 | A test change invokes known-channel verification and joins to identity/device evidence. |
| 5 | Staffing and supplier identity is controlled | E06 + ID-06 + ADM-03 | The provider record is independently verified and substitution routes to review. |
| 6 | Scoring can be piloted under governance | Part 3 case forms + escalation/response tiers | Two reviewers agree on evidence, root cause, tier and next action for a synthetic/retrospective case. |
| 7 | Recent hires can be reviewed as one population | Hunts 1 and 4 + case sheet | Findings are closed, investigated or converted into control changes. |

*Table 6. Developing outcomes and authoritative implementation path*

At this level, a reused address, device redirect and RMM alert become one case timeline rather than three unrelated facts.

**When am I ready to progress?**
You are ready to progress when the organisation can take a signal from any team, connect it to the same case, and agree the next proportionate verification step without jumping to conclusions about the candidate or employee.

# LEVEL 3: MATURE

**Best for:** organisations with a cross-functional insider-risk process, reliable telemetry and trained reviewers.

**Objective:** exploit the seams between application, interview, onboarding and employment, then calibrate the model against benign and adversarial scenarios.

**Implementation boundary. Do now: operate the governed scorecard, all four hunts, continuity testing and exercises.**

| ORDER | OUTCOME | IMPLEMENT THROUGH | PROOF |
|---|---|---|---|
| 1 | Cross-stage continuity is tested consistently | E03 Mature extension + COM-02/COM-04/COM-06 | Benign variation and a simulated handoff produce the intended different outcomes. |
| 2 | Simultaneous registered-channel control can be tested | E04 Mature extension + COM-05 | Benign failure is distinguished from repeated loss of channel control. |
| 3 | Corroboration gates govern escalation | Part 3 escalation sheet + response tiers | Correlated weak observations cannot create a critical decision by themselves. |
| 4 | Controlled canaries have a safe benign path | COM-01 and/or MIS-01 where approved | Benign interaction resolves correctly and an adversarial sequence is reviewable. |
| 5 | All four hunts operate on proved data | Part 2 Hunts 1-4 + E07 telemetry map | Each hunt has data, logic, owner, cadence and a passed acceptance test. |
| 6 | The score is calibrated before live use | Part 3 worked examples + response tiers | Benign and adversarial scenarios trigger the intended different response. |
| 7 | The organisation can exercise the response | Part 2 response + Part 3 escalation | Evidence preservation, containment and decision rights are executed within the agreed service level. |

*Table 7. Mature outcomes and authoritative implementation path*

Here the programme becomes threat-informed: each control is selected for the operating model it exposes, not because it appeared in a generic red-flag list.

**Ready to move up when:** the organisation can explain which attack model a control addresses, how it can fail, what evidence proves it operates and how the result changes the next decision.

# LEVEL 4: ADVANCED

**Best for:** organisations with established CTI, insider-risk, detection-engineering and data-correlation capability.

**Objective:** identify networks and handoffs at scale, including remote hardware and workers who may already be embedded

**Implementation boundary. Do now: automate correlation, emulate all five operating models and use intelligence to target fewer checks. Do not turn Advanced into "apply everything to everyone".**

| ORDER | OUTCOME | IMPLEMENT THROUGH | PROOF |
|---|---|---|---|
| 1 | Related personas and infrastructure are resolved at scale | E01/E06/E07 entities + ID-06 + correlation | A seeded facilitator cluster is surfaced with explainable links and human review. |
| 2 | Remote hardware is visible | DEV-03 + Hunt 2 | A representative IP-KVM event creates a case even when no EDR process is present. |
| 3 | Rotating operators can be distinguished from legitimate shifts | MIS-04 + E07 Advanced telemetry | Approved shared work is separated from unexplained identity rotation. |
| 4 | Cross-domain evidence creates one case | E07 telemetry map + case platform/hunts | Recruitment, identity, endpoint, data and Finance events join rather than alert separately. |
| 5 | The five operating models are emulated | Table 1 + Part 2 hunts + Part 3 readiness gates | The end-to-end trusted-referral scenario passes without bypassing prerequisite controls. |
| 6 | CTI changes the implemented controls | Threat-source review + hunt/control change process | A material TTP change produces a documented detection, control or training update. |
| 7 | Performance is measured without incentivising suspicion | Status dashboard + control-test/review metrics | Coverage, evidence quality, triage time, reviewer consistency and test outcomes are tracked. |

*Table 8. Advanced outcomes and authoritative implementation path*

Advanced capability means using stronger correlation to apply fewer, more targeted checks rather than applying every intrusive technique to every applicant.

**When am I ready to progress?**
You are ready to progress when the organisation can explain which attack model each control is designed to address, where that control might fail, what evidence shows it is working, and how the result should influence the next decision.

# USE THE SCORE TO CHOOSE THE NEXT CONTROL, NOT TO LABEL THE PERSON

The score exists to prevent weak observations from being lost between teams. It does not calculate the probability that a person is a DPRK operative.

> **When to use the score.** Foundation organisations should record facts but should not run the full scorecard live. Developing organisations should pilot it on a synthetic or retrospective case with a second reviewer. Mature and Advanced organisations may use it operationally after training, privacy review, accessible alternatives and a restricted case process are in place.

**The model groups evidence into six domains:**

1. identity and infrastructure;
2. communication continuity;
3. physical identity continuity;
4. device and access continuity;
5. mission and data behaviour; and
6. administration and finance.

**Five rules keep the model defensible:**

- **Score observable facts, not attributes.** Accent, nationality, grammar, local knowledge and gut feeling do not add points.
- **Count one root cause once.** A single connectivity issue should not create three separate scores.
- **Use fixed signal weights.** A +3 signal scores 0 or +3, never +1 or +2; award it only when the stated scoring condition is met.
- **Require corroboration.** Weak signals should span independent domains or stages before they raise the response tier.
- **Keep the decision human-led.** The score selects the next verification or investigation step. It does not automatically reject, dismiss or report anyone.

| MATURITY | PERMITTED SCORE USE | PRECONDITIONS | AUTHORITATIVE REFERENCE |
|---|---|---|---|
| **FOUNDATION** | Record facts only; do not operate the full score live. | Current-maturity controls are configured and acceptance-tested. | Part 3 stage forms and escalation rules. |
| **DEVELOPING** | Pilot on synthetic or retrospective evidence with a second reviewer. | Restricted case process, trained reviewers and coverage review exist. | Part 3 response tiers and worked examples. |
| **MATURE** | Live human-led use after the go-live gate passes. | Universal prerequisites pass; enabled rows are ready or formally out of scope; bands are reviewed for coverage. | Part 3 Table 26 — Response-tier quick reference. |

| MATURITY | PERMITTED SCORE USE | PRECONDITIONS | AUTHORITATIVE REFERENCE |
|---|---|---|---|
| Advanced | Same human-led score governance as mature; automate correlation, not adverse employment decisions. | Explainable correlation, data quality, privacy controls and human review are proved. | Part 3 Table 26 — Response-tier quick reference. |

*Table 9. Score use by maturity — operational thresholds are authoritative in Part 3*

Operational thresholds and response gates are authoritative only in Part 3. Before live scoring, review the enabled check set for actual coverage; do not lower thresholds mechanically to compensate for missing controls. During the first year, review false positives, thresholds and reviewer consistency quarterly.

# PART 2 — DETECT AND RESPOND

## FOUR PRIORITY HUNTS FOR SOC AND INSIDER-RISK

Recruitment controls can fail. The post-hire layer should assume that a DPRK IT worker operation may already control valid credentials and a compliant endpoint. These four hunts follow the operation from hidden control of the device, through conflicts between device and identity, into collection or outsourced delivery, and finally into identity or payment changes that may indicate a handoff.

> **Run only the hunts your maturity supports.** Foundation: Hunt 1. Developing: Hunts 1 and 4. Mature: all four hunts. Advanced: automate cross-domain correlation and add remote-hardware coverage. Before assigning any hunt, confirm that every item in “Required data” is available, retained and legally usable. For BYOD-to-VDI, record missing host telemetry and do not assign an endpoint-dependent hunt unless equivalent VDI, identity or network sources satisfy its required data.[2][18]

Practitioner case studies have highlighted remote-access chaining, secondary virtual private networks, persona-management tooling, translation services, trusted-referral chains and outsourced task delivery as useful hunt hypotheses. Treat them as starting points to test against the organisation's own baseline, not as standalone indicators.[12][14][15]

---

## HUNT 1: REMOTE-CONTROL CHAINING, UNAUTHORISED VIRTUAL PRIVATE NETWORKS AND HIDDEN ACCESS

**REQUIRED DATA:** device or VDI provisioning date, user-to-endpoint/VDI mapping, EDR process, command-line and service telemetry, software inventory, network connections, VPN client inventory, web proxy data, security-control health/configuration events where available, and support tickets.

**LOGIC:** an in-scope endpoint or VDI less than 90 days old rapidly downloads or attempts to install several remote-access or screen-sharing tools until one succeeds; uses sequential or concurrent remote-control mechanisms; runs a secondary VPN; or establishes persistent remote-control, tunnelling, browser-extension or virtual-camera activity. Increase priority when this follows first-day host/system discovery, public-IP/location checking, policy-inconsistent personal-account/browser activity, or attempts to disable or bypass endpoint, SASE, proxy or access controls. These precursor behaviours do not score alone. Treat failed and blocked attempts as part of the chain, not as harmless noise.[15][18]

**TRIAGE:** confirm whether each tool is approved; inspect signer, command line, parent process, persistence, sequence and destination; determine whether security controls were disabled or bypassed; identify residential proxy or VPN infrastructure; then connect the activity to delivery/VDI and recruitment evidence.

**ACCEPTANCE TEST:** a permitted support tool is suppressed correctly, while seeded host/IP discovery followed by blocked and successful remote-access attempts plus an unauthorised VPN creates one case with new-hire context; where control-health telemetry exists, a seeded disable/bypass event joins the same case.

---

## HUNT 2: DEVICE, MULTIFACTOR AUTHENTICATION AND LOCATION DO NOT AGREE

**REQUIRED DATA:** network access control (NAC), switch and Dynamic Host Configuration Protocol (DHCP) logs, Universal Serial Bus (USB) and peripheral telemetry, asset/VDI inventory, identity-provider sign-ins, MFA/authentication-factor device telemetry where available, HR address records and physical support records.

**LOGIC:** a newly issued endpoint is associated with an unexpected USB network interface, keyboard-video-mouse device, management endpoint or persistent connection pattern consistent with remote hardware; the endpoint or VDI session differs materially from the MFA/authentication-factor device or expected access context; session evidence suggests multiple operators; or a residential proxy appears domestic but does not align with the employee address held by HR. Successful MFA alone does not establish identity continuity because codes or approvals can be relayed.[15]

**TRIAGE:** confirm docking stations, accessibility equipment, keyboard-video-mouse (KVM) devices and support equipment. Compare the primary session, managed endpoint or VDI, authentication factor/device and registered working context; then review the physical device and local network where possible. Treat OTP/MFA success as one event, not proof that the same person controls the session.

**ACCEPTANCE TEST**: a representative Internet Protocol keyboard-video-mouse (IP-KVM) event, seeded endpoint/VDI-versus-factor mismatch or simulated relay scenario is visible even though no RMM process exists on the endpoint.

---

## HUNT 3: REPOSITORY COLLECTION, EXTERNAL ASSISTANCE AND LARGE LANGUAGE MODEL USE

**REQUIRED DATA:** Git or Azure DevOps audit data, data loss prevention (DLP), secure web gateway or proxy logs, approved large language model (LLM) service audit logs, cloud-storage, email and endpoint file telemetry.

**LOGIC:** a new starter bulk-clones repositories, accesses secrets or projects outside the assigned role, then transfers data to a personal account, external fork, cloud service, USB device or unauthorised destination. Correlate this with policy-inconsistent or unauthorised use of LLM or GPT-style services, repeated translation between unexpected languages, prompts asking for unfamiliar code to be explained or rewritten, uploads of internal documentation, and sustained traffic to freelance marketplaces such as Fiverr or equivalent services that may indicate outsourced delivery.[12]

**TRIAGE:** validate onboarding, build, backup and migration activity with the manager. Review prompt content only where monitoring is lawful, proportionate and authorised. Prioritise destination, sequence, internal-document uploads, translation patterns and requests inconsistent with the assigned role; high LLM usage alone is not suspicious for many developers. Do not assume that absence of cloud-LLM logs rules out AI assistance: local or off-platform use may leave no enterprise AI-service record, so behaviour and data movement remain primary.[16]

**ACCEPTANCE TEST**: a test bulk clone followed by controlled upload of a marked internal document to an approved test LLM service produces one joined case rather than separate low-context alerts.

---

# HUNT 4: IDENTITY DRIFT, WORK SIMULATION AND ADMINISTRATIVE CHANGE

**REQUIRED DATA:** identity provider (IdP) sessions, managed-device identity, HR and payroll changes, endpoint software and configuration inventory, equipment records, live check-in outcome and collaboration logs.

**LOGIC:** an early payment, address or contact change coincides with a new device, unexplained session, working-pattern shift or failed post-onboarding identity check. Add unexpected Mandarin or Korean language packs, keyboard layouts, repeated translation tooling and mouse-jiggler scripts or software used to simulate activity as corroborating—not standalone—signals.

**TRIAGE**: verify the administrative change through the established channel, establish whether language settings have a legitimate business or accessibility explanation, review the purpose of any activity-simulation tooling, then assess whether the person, device, account and payment identity remain bound together.

**ACCEPTANCE TEST**: a legitimate payroll or language-setting change is resolved through verification, while a simulated handoff with mouse-jiggler activity and an unexplained account change creates a multi-team case.

# RESPOND WITHOUT LOSING CONTROL OF THE INVESTIGATION

When a case crosses the high-concern or critical threshold, the organisation should move from screening to coordinated insider-risk response.

1. **PRESERVE THE EVIDENCE.** Retain the approved interview, case, identity, delivery, endpoint, repository, email and payment records. Do not collect more than policy allows.
2. **CONVENE THE RIGHT FUNCTIONS.** Security, HR, Legal, the Data Protection Officer (DPO) and sanctions compliance should agree the investigation and decision owner.
3. **ASSESS IMMEDIATE HARM.** Active exfiltration or confirmed remote control may require rapid containment. Where there is no imminent harm, avoid alerting the subject before evidence and containment are ready.
4. **RECONSTRUCT THE ACCESS PATH.** Determine who received the device, how it was controlled, what systems and secrets were accessed, and what data may have left.
5. **CONTAIN AND RECOVER.** Revoke access, retrieve the device through an approved route, rotate exposed credentials and secrets, and review related applicants, hires and suppliers.

   **Remote-control exposure rule.** Where unauthorised remote control, screen control or screen sharing is established, treat sensitive information and secrets displayed during affected sessions as potentially exposed even when DLP or file-transfer telemetry shows no transfer. Scope credential/secret rotation and data-impact assessment accordingly.[18]
6. **TAKE LEGAL AND REPORTING ADVICE.** Assess sanctions and law-enforcement reporting with counsel and the appropriate authorities.

The response should not depend on proving nationality. It should depend on verified identity substitution, unauthorised control, policy breach, data access or other evidence relevant to the employment and security decision.

# WHAT NOT TO OVER-TRUST

Some cues may provide context but should not drive the programme or score by themselves. Part 3 contains the authoritative no-score list for live use.

| CUE CATEGORY | OPERATIONAL RULE |
|---|---|
| **LANGUAGE, CULTURAL OR DEMOGRAPHIC CUES** | Accent, grammar, nationality, local knowledge, timezone hesitation or language settings are heavily confounded and create equality risk. Political or loyalty questions are not required. |
| **AI, TRANSLATION AND SYNTHETIC-MEDIA CUES** | AI or translation use, a single canary, deepfake artefacts, document appearance or metadata do not establish identity or control. Use only as contextual evidence. |
| **NETWORK AND ENVIRONMENT CUES** | IP geolocation, visible latency, video background, sockets or similar environmental details are confounded by VPN, VDI, travel and ordinary technical variation. |
| **VISUAL OR PHYSICAL INTUITION** | Handwriting, appearance or manner judged informally is unreliable. Use only approved repeatable continuity methods with independent evidence and accessibility safeguards. |
| **AUTHENTICATION SUCCESS** | Successful OTP/MFA proves an authentication event or channel interaction, not that the same person controls the session. Correlate factor/device, endpoint-or-VDI and session context. |

*Table 10. Decaying cues — why they should not drive the programme*

**We assess that five control families will retain value as AI improves:**

- cross-stage identity continuity;
- simultaneous control of independent channels;
- device and remote-hardware integrity;
- entity reuse across applicants, hires and suppliers; and
- mission-behaviour detection, including collection and exfiltration.

The investment principle is straightforward: **fund controls that test the operating model, not the current imperfections of a deepfake.**

# CONCLUSION: MAKE THE OPERATION PRESERVE CONTINUITY

DPRK IT worker operations succeed because legitimate business processes create trust in stages: application, interview, offer, device, account and access.

A strong defence uses the same stages to make the operation preserve continuity.

For a less mature organisation, that starts with the minimum viable four and one tested case process. A developing organisation connects HR, security, finance and supplier evidence before piloting the score. A mature programme adds cross-stage tests, all four hunts and calibrated review. An advanced programme automates entity correlation, detects remote hardware and exercises the threat as it evolves. Progress is evidence-led, not calendar-led.

The objective is not to identify people from North Korea or to treat nationality as suspicious. It is to detect evidence that a DPRK IT worker operation has placed, substituted or remotely controlled an insider identity within the organisation, and to make laptop farms, persona relays and hidden remote access harder to maintain.

Start with one in-scope role, one recent hire and one tested hunt. The goal is not to build suspicion into hiring; it is to stop trusted access being handed across an unverified seam.

# PART 3 — OPERATIONAL WORKBOOK

Use this section to set up and then operate a live or retrospective case. Do not begin with the forms: complete the universal prerequisites, follow the numbered set-up tasks for each in-scope check and mark only proven checks Ready. Then complete the case sheet once, open only the current-stage form, record evidence once and escalate only when triggered.

**Workbook navigation:** Status | Set-up plan | Case sheet | Application | Phone screen | Interview one | Interview two | Onboarding | First 90 days | Escalation | Signal library

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Complete the case sheet once | Open only the current stage | Record evidence once | Update cumulative position | Escalate only when triggered |

**RESULT CODES | NC = no concern | EXP = explained | OPEN = unresolved and the scoring condition is met | N/A = not applicable.**

Enter points only for OPEN rows whose stated condition is satisfied.
FIXED-WEIGHT RULE | Signal weights are not ranges. A +3 signal scores 0 or +3, never +1 or +2. Award the full stated weight only when the scoring condition is met. If evidence is incomplete, leave the row unscored and keep the follow-up open.

## IMPLEMENTATION STATUS — ONE-PAGE PROGRAMME VIEW

Use this page to run the implementation. Click an item in the first column to jump to its definition or setup section. **Accountability rule:** one function owns readiness; supporting teams are shown in the detailed setup rows.

| WHAT MUST BE READY | ACCOUNTABLE OWNER | STATUS | NEXT ACTION / DUE DATE |
|---|---|---|---|
| Universal prerequisites | Programme Owner | ☐ Ready ☐ Blocked | _____ |
| Applicant identity and contact record [E01] | HR Recruitment Operations | ☐ Ready ☐ Blocked | _____ |
| Approved live identity/liveness process [E02] | HR Recruitment Operations | ☐ Ready ☐ Blocked | _____ |
| Interview baseline and continuity methods [E03] | HR Recruitment Operations | ☐ Ready ☐ Blocked | _____ |
| Registered-channel control verification [E04] | IAM / Identity Services | ☐ Ready ☐ Blocked | _____ |
| Equipment delivery and device custody [E05] | IT Logistics | ☐ Ready ☐ Blocked | _____ |
| HR, payroll, payment and supplier continuity [E06] | HR Operations | ☐ Ready ☐ Blocked | _____ |
| New-hire security context, access binding and telemetry [E07] | SOC / Security Operations | ☐ Ready ☐ Blocked | _____ |
| Application stage | HR Screening Coordinator | ☐ Ready ☐ Blocked | _____ |

| WHAT MUST BE READY | ACCOUNTABLE OWNER | STATUS | NEXT ACTION / DUE DATE |
|---|---|---|---|
| Phone-screen stage | HR Screening Coordinator | ☐ Ready ☐ Blocked | _____ |
| Interview 1 stage | Hiring Manager | ☐ Ready ☐ Blocked | _____ |
| Interview 2 stage | Round-two Chair | ☐ Ready ☐ Blocked | _____ |
| Onboarding stage | HR Operations | ☐ Ready ☐ Blocked | _____ |
| First 90 days | SOC / Security Operations | ☐ Ready ☐ Blocked | _____ |
| Scorecard coverage reviewed | Programme Owner | ☐ Ready ☐ Blocked | _____ |
| **Live scoring authorised** | **Programme Owner** | **☐ YES ☐ NO** | _____ |

# BEFORE LIVE USE: UNIVERSAL PREREQUISITES

Do not score a live candidate or employee until every prerequisite below is in place. Use the workbook for a tabletop or retrospective review while any item remains incomplete.

| *READY* | PREREQUISITE | EVIDENCE |
|---|---|---|
| ☐ | A named programme owner and documented in-scope roles | Owner, scope and decision rights approved |
| ☐ | One restricted case record with controlled access | Access and audit controls tested |
| ☐ | Privacy, employment, equality and sanctions review | Approved legal and policy position |
| ☐ | Evidence retention and deletion rules | Retention period and deletion owner recorded |
| ☐ | Accessible alternatives for live verification | Alternative routes documented and briefed |
| ☐ | Trained operators and a second-review route | Training completed and reviewer named |
| ☐ | A tested escalation and containment process | Synthetic case completed end to end |
| ☐ | Maturity-appropriate telemetry for post-hire checks | Required data is available and legally usable |
| ☐ | Every in-scope stage check at or below the current maturity level is configured and acceptance-tested | The matching setup rows below are marked ready; unsupported or higher-maturity checks are disabled and shown as N/A |
| ☐ | Enabled check set and response-tier bands reviewed for actual coverage | Current maturity, deliberate exclusions and enabled weighted checks recorded; bands approved before live scoring |

**DO NOT SCORE THESE OBSERVATIONS**

They may justify a neutral follow-up question, but they do not add points by themselves.

| | |
|---|---|
| • Accent, grammar, spelling, name, nationality or ethnicity | • Country-code or timezone hesitation |
| • Knowledge of UK tax, pensions, local venues or cultural trivia | • One forgotten breadcrumb or one uncorrected typo |
| • AI use, translation use or a language pack alone | • Power sockets, packaging or background details seen on video |
| • Visual deepfake artefacts without independent confirmation | • Keystroke latency without endpoint or network evidence |
| • Refusal to make a political statement or criticise a government | • An assessor's gut feeling without a describable fact |

# HOW TO USE THE SETUP DEPENDENCIES

**For every check, work in this order:**

1. Read **Required** first
2. Follow any missing dependency and build or record it
3. Complete **Set up** this check in order;
4. Run the **Ready when test**. Do not activate a check while it is blocked.

**Dependency labels:** BUILD ONCE = an organisational capability reused across hires. STAGE BASELINE/EARLIER STAGE = candidate-specific evidence created earlier. EARLIER CHECK = the same approved method or result is intentionally reused. A dependency is on the capability or evidence, not on a previous score.

**BUILD-ONCE CONTRACT |** A BUILD ONCE capability is ready only when it produces the reusable template, method, dataset or record named in its row. A downstream setup row may apply or configure that output; it must not be the first place that the reusable method, field, threshold or evidence rule is invented.

**MATERIALITY RULE |** A difference is material only when it is objectively evidenced, tied to a defined source or baseline, survives reasonable clarification and benign explanations, and is significant to identity continuity, ownership, access or control. Record why it is material.

# BUILD ONCE: SHARED CAPABILITIES

Establish these reusable capabilities before the individual rows that reference them. Where a capability supports checks at different maturity levels, build the basic capability first and enable only the advanced method required by the row at its stated maturity. One accountable function owns readiness for each capability; the support functions contribute delivery and assurance.

| BUILD-ONCE CAPABILITY | ACCOUNTABLE OWNER / SUPPORT | MINIMUM SETUP SEQUENCE | READY WHEN | SET-UP EFFORT | MINIMUM MATURITY |
|---|---|---|---|---|---|
| ***E01 - Applicant identity and contact record*** | **Accountable:** HR Recruitment Operations<br>**Support:** HRIS | **Produces:** Applicant Identity and Contact Record (canonical intake record).<br>**1. Decide once:** Define declared/canonical identity, registered phone/email, residential/working/proposed delivery address, application source, referral/introducer/internal sponsor plus stated relationship, role, and a provenance/status field for each value. E01 records what was supplied or registered; it does not by itself prove that every field is independently verified.<br>**2. Implement once:** Store the record in the ATS/restricted process, normalise fields used for matching, retain correction/exception history, and identify which later capability creates a verified result: E02 for person/identity, E05 for delivery destination/recipient and E06 for supplier/payment continuity.<br>**3. Test once:** Create, correct and retrieve a seeded applicant record from a later stage. | **Ready when:** The same canonical record and provenance are retrievable and auditable, and downstream rows can use the defined fields without inventing a new intake record. | Medium | Foundation |
| ***E02 - Approved live identity/liveness process*** | **Accountable:** HR Recruitment Operations<br>**Support:** Security, Legal, DPO, identity provider | **Produces:** Identity/Liveness Standard + candidate Identity Result Record.<br>**1. Decide once by stage:** Document the approved method/provider/source, liveness requirement, result states (Complete / Exception / Unresolved), fields retained and exact comparison target. The method matrix must state: Interview 1 -> live-person baseline; Onboarding -> compare with Interview 1; weeks 2/3 -> compare with Interview 1 and onboarding. Visual inspection of an identity document alone is not verification.[15]<br>**2. Govern once:** Define accessible alternatives, authorised reviewers, evidence/retention, correction/appeal and mismatch route; specify the fields used to bind the result to Interview baseline and continuity methods [E03].<br>**3. Test once:** Run a normal result, an approved exception and an unresolved mismatch. | **Ready when:** Each stage has an approved method, result schema and comparison target, and downstream PHY checks can retrieve the exact result without choosing or designing the method themselves. | High | Foundation |
| ***E03 - Interview baseline and continuity methods*** | **Accountable:** HR Recruitment Operations | **Produces:** Interview Baseline Template + Continuity Method Standard. | **Ready when:** The baseline template and enabled method | Medium | Foundation |

| | | | | | |
|---|---|---|---|---|---|
| | **Support:** Hiring Manager, DPO | **1. Foundation minimum:** Define the Interview 1 baseline fields: panel/date, E02 result reference, working context, material technical statements, permitted notes/recordings, storage/access/retention and secure retrieval.<br><br>**2. Mature extension - decide before enabling continuity checks:** Breadcrumbs - approved bank/selection/rotation rule; at least two unique non-essential details per test; proof of delivery; exclude personal, political, cultural or protected-characteristic trivia; one miss never scores. Callback - permitted material, non-political statements; original statement recorded; inaccurate restatement plus fair correction opportunity and evidence fields. Physical prompt - approved low-risk prompt(s), notice/accessibility alternative and minimal evidence; no forensic handwriting or biometric interpretation.<br><br>**3. Test once:** A later panel retrieves the baseline and runs every enabled method against one benign and one mismatch scenario. | standards are approved and repeatable; downstream COM-02, COM-04 and PHY-04 can apply them without inventing wording, evidence rules or thresholds. | | |
| ***E04 - Registered-channel control verification*** | **Accountable:** IAM / Identity Services<br><br>**Support:** HR, DPO | **Produces:** Registered-channel Verification Procedure + First-90-day Recovery Procedure.<br><br>**1. Developing minimum:** Use the Applicant identity and contact record [E01] registered phone/email as authoritative channels. Define known-channel verification for administrative changes, MFA reset/re-enrolment and account recovery: initiator, fresh challenge, time window, retries, accessible alternative, minimum evidence and the route when a channel is unavailable. Never rely only on the factor being replaced.[19]<br><br>**2. Mature extension:** Define the simultaneous two-channel COM-05 method once: participant remains on camera; separate fresh random challenges are sent to phone and email; define success/failure window, retries and minimum logging. Success proves channel control only, not person/device identity.<br><br>**3. Test once:** Run benign delivery failure, genuine loss-of-control and factor-recovery scenarios; when the Mature method is enabled, also test simultaneous success and failure. | **Ready when:** COM-05, ADM-01 and DEV-04 can execute the relevant maturity method without designing the channel-control or recovery procedure at the point of use. | Medium | Developing |
| ***E05 - Equipment delivery and device custody*** | **Accountable:** IT Logistics<br><br>**Support:** HR | **Produces:** Delivery Verification and Custody Standard + Device Delivery/Custody Record.<br><br>**1. Decide once:** Use the canonical person/address fields from Applicant identity and contact record [E01] as the starting record. Before shipment, define the approved route that verifies or approves the delivery destination and named recipient, record the verification source/date, and bind a unique device identifier. The E01 address alone is not a verified delivery destination.<br><br>**2. Govern once:** Define redirect, forwarding, third-party collection and address-change approval; chain-of-custody fields; exception owner; and recovery/return route.<br><br>**3. Test once:** Run a normal shipment plus a redirect or third-party collection and retrieve the complete device-recipient history. | **Ready when:** For each physical device the organisation can evidence the authorised person, approved destination, named recipient, device ID and custody/exception history; downstream ID-07 does not need to invent delivery verification. | Medium | Foundation |

| | | | | | |
|---|---|---|---|---|---|
| ***E06 - HR, payroll, payment and supplier continuity*** | **Accountable:** HR Operations<br>**Support:** Finance, Procurement | **Produces:** Supplier Verification Record + HR/Payment Continuity Field Map.<br>**1. Supplier verification record:** For in-scope staffing, outsourced-development and technology suppliers record the legal-entity identifier, independent/official source used, registered address, corporate/domain presence, independently sourced authorised contact, contract/named worker, subcontractor declaration, reviewer/date and outcome before approval; do not rely only on the supplier website or supplied references.[17]<br>**2. Continuity field map:** Define the authoritative identifiers/fields shared across HR, payroll, payment and the verified supplier record, plus correction/second-channel verification, substitution/subcontractor approval and restricted access.<br>**3. Test once:** Run a supplier-identity mismatch and a worker/subcontractor substitution. | **Ready when:** The supplier record is independently traceable and complete, continuity fields reconcile to the same person/entity, and ID-06/ADM-03 can consume the record without defining supplier verification themselves. | High | Developing |
| ***E07 - New-hire security context, access binding and telemetry*** | **Accountable:** SOC / Security Operations<br>**Support:** IAM, Endpoint, Network, Data Security | **Produces:** New-hire Security Context Template + Work/Access Baseline Template + Enabled-check Telemetry Map.<br>**1. Foundation minimum:** Before first login define the user/account/managed-endpoint-or-VDI binding and, where supported, enrolled factor/device; define work/access fields for role, team, manager, approved systems/repositories, initial entitlements, expected task/data scope, authorised destinations and exceptions; define the access-review schedule.<br>**2. Map every enabled check:** For each check at or below the current maturity record check ID, required source/event/fields, join key, retention, owner, lawful-use status, visibility gap/equivalent VDI-identity-network source, seeded test event and Ready/Blocked/Out of scope status. Developing adds IdP/MFA/recovery/admin data; Mature adds repository/DLP/cloud/web data; Advanced adds remote-hardware/cross-domain data. Link first-90-day recovery to Registered-channel control verification [E04]. Where BYOD reaches VDI, unavailable host evidence must be explicit.[2][18]<br>**3. Test once:** Run the recorded test event for every enabled check before live use and test one BYOD-to-VDI visibility gap where relevant. | **Ready when:** The binding and work/access templates exist, every enabled check has a complete tested telemetry-map row, and any unsupported check remains Blocked or formally Out of scope. | High | Foundation |

**Stage evidence chain:** Application baseline -> Phone-screen baseline -> Interview 1 baseline -> Interview 2 continuity record -> Onboarding baseline -> First-90-days baseline. Later checks may reuse these outputs; they never depend on a previous score.

# STAGE ROUTING AND SETUP READINESS — BUILD EACH CHECK BEFORE YOU USE IT

Read each stage from top to bottom. The required first column shows the dependency that must already exist; the numbered tasks are only the additional work needed to enable that check.

Setup status: Ready = all dependencies exist and the readiness test passed. Blocked = one or more dependencies are missing. Out of scope = deliberately excluded by approved maturity or programme scope. A Blocked row is a programme gap, not evidence about a candidate or employee.

Maturity identifies when a capability should be built; it does not authorise live scoring. Foundation records facts, Developing pilots the score, and Mature/Advanced may score live only after the universal prerequisites pass.

| STAGE | ACCOUNTABLE STAGE OWNER | SET-UP PLAN | USE THIS SECTION TO | CLOSE THE STAGE WHEN |
|---|---|---|---|---|
| *Application* | HR Screening Coordinator | Open setup | Complete duplicate, identity and contact checks. | Checks are complete and unresolved facts have an owner. |
| *Phone screen* | HR Screening Coordinator | Open setup | Create the communication and factual-ownership baseline. | Material differences have an explanation or follow-up. |
| *Interview one* | Hiring Manager | Open setup | Create the live identity and working-context baseline. | The permitted baseline and open facts are recorded. |
| *Interview two* | Round-two Chair | Open setup | Test cross-round continuity and channel control. | Unresolved signals and next action are recorded. |
| *Onboarding* | HR Operations | Open setup | Bind person, recipient, account, supplier and payment. | Access is released only when mismatches are resolved or approved. |
| *First 90 days* | SOC / Security Operations | Open setup | Establish the work/access baseline, then complete re-verification and maturity-appropriate telemetry checks. | Findings are closed or escalated. |

*Table 11. Stage routing and close conditions*

# STAGE 1 — APPLICATION REVIEW: SET-UP SEQUENCE BEFORE USE

Before you set up this stage: complete the universal prerequisites and Applicant identity and contact record [E01]. Equipment delivery and device custody [E05] must be ready before ID-03 uses delivery history; HR, payroll, payment and supplier continuity [E06] must be ready before ID-06 uses supplier records.

| STATUS | CHECK AND SCORE CONDITION | REQUIRED FIRST | MINIMUM TASKS TO ENABLE THIS CHECK | SETUP EFFORT | MINIMUM MATURITY |
|---|---|---|---|---|---|
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **Required baseline (0 points)**<br>**Check:** Confirm the application source, role, declared identity, contact details, proposed equipment-delivery address and, where applicable, referral/introducer/internal sponsor.<br>**Record:** *Record completion and route any objective discrepancy to the relevant signal below.* | UNIVERSAL: Live-use prerequisites<br>BUILD ONCE: Applicant identity and contact record [E01] | **Delivery:** HR Recruitment Operations<br>Set up this check<br>1. Use E01 as the mandatory intake record for every in-scope applicant; referral, internal sponsorship, urgency or supplier recommendation does not waive the standard baseline.<br>2. Capture application source, role, working location, proposed delivery address and any referral/introducer/internal sponsor plus stated relationship alongside the authoritative identity and registered contact fields.<br>3. Route any missing or conflicting field to the named exception owner and test one application end to end.<br>Ready when: A test application uses the same authoritative fields and an objective discrepancy creates a named follow-up. | Low | Foundation |
| ☐ Ready<br>☐ Blocked | **ID-01 (+1)** | STAGE BASELINE: Application baseline | **Delivery:** HR Recruitment Operations + Privacy<br>Set up this check<br>1. Approve the carrier/VoIP lookup method and its permitted use. | Low | Foundation |

| | | | | | |
|---|---|---|---|---|---|
| ☐ Out of scope | **Check:** Run the approved carrier lookup on the declared primary number where policy permits.<br>**Score when:** *the result is verified as VoIP. VoIP use alone is not suspicious.* | | 2. Define where the result is recorded and which independent channel is used to confirm control.<br>3. Test known VoIP and non-VoIP numbers.<br>Ready when: The lookup is reproducible, retained appropriately and never treated as adverse evidence by itself. | | |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ID-02 (+3)**<br>**Check:** Search the applicant tracking system across active applications and recent hires for the same phone number or email.<br>**Score when:** *apparently unrelated identities share the contact point and household, agency or data-entry explanations are excluded.* | STAGE BASELINE: Application baseline | **Delivery:** HRIS / ATS owner + Security<br>Set up this check<br>1. Define the applicant/recent-hire lookback population and normalise phone and email values used for matching.<br>2. Document legitimate household, agency and data-entry exceptions.<br>3. Assign the linked-record review owner and test seeded duplicates.<br>Ready when: Seeded duplicate phone and email records are surfaced with linked records and an owner. | Medium | Foundation |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ID-03 (+4)**<br>**Check:** Compare residential and proposed delivery addresses across applicants and recent hires.<br>**Score when:** *the same address appears across unrelated identities with no credible relationship.* | STAGE BASELINE: Application baseline<br>BUILD ONCE: Equipment delivery and device custody [E05] | **Delivery:** HRIS / ATS owner + IT Logistics<br>Set up this check<br>1. Join the application address fields to the E05 delivery history and define the lookback population.<br>2. Document legitimate shared-housing and supplier exceptions and make prior device deliveries visible.<br>3. Test a seeded shared address across unrelated identities.<br>Ready when: The shared address is detected and routed for recipient and delivery-history review. | Medium | Foundation |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ID-04 (+2)**<br>**Check:** Compare dates, names, education and employment claims across the application and approved verification sources.<br>**Score when:** *a material conflict remains after the applicant has a fair opportunity to correct or explain it.* | STAGE BASELINE: Application baseline | **Delivery:** HR + Screening provider<br>**Set up this check**<br>**1.** List the approved verification sources, apply the global materiality rule and document check-specific examples for identity, education and employment conflicts.<br>**2.** Define the candidate correction/explanation route and the evidence that may be retained.<br>**3.** Test a synthetic identity, education or employment conflict.<br>**Ready when:** The conflict can be evidenced, linked to its source, explained/corrected or left open without relying on intuition. | Medium | Developing |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ID-05 (+3)**<br>**Check:** Where references occur at this stage, source the organisation or referee independently rather than using only candidate-provided details.<br>**Score when:** *the referee or employer cannot be validated through an independently sourced route after reasonable attempts.* | STAGE BASELINE: Application baseline | **Delivery:** HR + Screening provider<br>Set up this check<br>1. Define the independent reference-verification channels: corporate domain, switchboard or trusted provider.<br>2. Set the reasonable-attempt threshold and the route for an unresolved reference.<br>3. Test a reference without using only candidate-supplied contact details.<br>Ready when: A valid referee can be independently verified and an unresolved result is held open correctly. | Medium | Developing |

| | | | | | |
|---|---|---|---|---|---|
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ID-06 (+3)**<br>**Check:** Check whether an agency, referee, referral/introducer/internal sponsor, domain or contact point appears across several apparently unrelated candidates.<br>**Score when:** *a repeated cluster cannot be explained by an approved supplier or shared service.* | STAGE BASELINE: Application baseline<br>BUILD ONCE: HR, payroll, payment and supplier continuity [E06] | **Delivery:** HR + Procurement + Security<br>Set up this check<br>1. Choose the agency, referee, referral/introducer/internal sponsor, domain and contact fields to compare and use the E06 approved-supplier record.<br>2. Give the reviewer access to the relevant candidate and supplier/contract records.<br>3. Assign a manual link-review owner and test a seeded cluster.<br>Ready when: A repeated cluster is surfaced, legitimate supplier reuse is explained and unresolved links are assigned. | High | Developing (Advanced to automate) |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-01 (+1)**<br>**Check:** Only where approved, rotate an accessible and policy-reviewed automation canary across separate communications.<br>**Score when:** *two or more triggers occur after mail-system artefacts and assistive-technology explanations are excluded.* | UNIVERSAL: Live-use prerequisites<br>STAGE BASELINE: Application baseline | **Delivery:** HR + Security + DPO<br>Set up this check<br>1. Approve the automation-canary wording, rotation and accessible alternative.<br>2. Test mail-system and assistive-technology effects; set the trigger threshold and retention rule.<br>3. Define the human review route and prohibit automatic adverse decisions.<br>Ready when: Benign artefacts are excluded while repeated automated reproduction creates a reviewable observation. | High | Mature |

*Table 12. Application stage: dependencies and minimum setup before each check can be used*

# STAGE 2 — PHONE SCREEN: SET-UP SEQUENCE BEFORE USE

Before you set up this stage: the Application baseline is retrievable and Applicant identity and contact record [E01] is ready. Interview baseline and continuity methods [E03] must be ready before continuity prompts or factual-ownership comparison are enabled.

| STATUS | CHECK AND SCORE CONDITION | REQUIRED FIRST | MINIMUM TASKS TO ENABLE THIS CHECK | SETUP EFFORT | MINIMUM MATURITY |
|---|---|---|---|---|---|
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **Required baseline (0 points)**<br>**Check:** Confirm the participant's name, role, registered phone and email, and ask them to summarise the material application in their own words.<br>**Record:** *Record who participated, the channels used and any explanation for differences.* | STAGE BASELINE: Application baseline<br>BUILD ONCE: Applicant identity and contact record [E01] | **Delivery:** HR screener / Hiring manager<br>Set up this check<br>1. Create the standard phone-screen script and note template using the Application baseline.<br>2. Record the participant, registered channels and material application summary in the restricted record so the next stage can retrieve them.<br>3. Run one mock phone screen.<br>Ready when: The mock produces a complete Phone-screen baseline that the next panel can retrieve. | Low | Foundation |
| ☐ Ready<br>☐ Blocked | **ID-04 (+2)**<br>**Check:** Revisit one or two objective education, employment or role details already supplied in the application. | STAGE BASELINE: Application baseline<br>STAGE BASELINE: Phone-screen baseline | **Delivery:** HR<br>**Set up this check**<br>**1.** Give the screener access to the Application baseline and approved verification results. | Medium | Developing |

| | | | | | |
|---|---|---|---|---|---|
| ☐ Out of scope | **Score when:** *a material conflict remains after a clear and fair prompt; normal memory variation is not scored.* | | **2.** Apply the global materiality rule to fair factual prompts and use the existing correction/explanation route; normal memory variation remains non-scoring.<br>**3.** Test a mock material discrepancy.<br>**Ready when:** The source, exact discrepancy, explanation, materiality rationale and next verification step are recorded. | | |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-02 (+2)**<br>**Check:** Where approved, ask about two non-essential details previously sent to the registered account.<br>**Score when:** *multiple details are not known after confirming the correspondence reached the correct account.* | STAGE BASELINE: Application baseline<br>BUILD ONCE: Interview baseline and continuity methods [E03] | **Delivery:** HR + Hiring manager + DPO<br>**Set up this check**<br>**1.** Use the E03-approved breadcrumb standard plus its bank/selection/rotation rule to choose at least two candidate-specific non-essential details; record proof of delivery to the registered account.<br>**2.** Apply the two-miss rule, accessible alternative and prohibition on personal, political, cultural or protected-characteristic trivia.<br>**3.** Test delivery, recall and recording using one benign and one mismatch scenario.<br>**Ready when:** The check can be run without inventing breadcrumbs at the point of use, scoring one miss or treating a delivery problem as a signal. | Medium | Mature |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-03 (+2)**<br>**Check:** Confirm that the person can use the registered phone and email and understands the current process and appointment.<br>**Score when:** *objective evidence suggests different people control the channels or the participant lacks material context from registered communications.* | STAGE BASELINE: Application baseline<br>STAGE BASELINE: Phone-screen baseline | **Delivery:** HR<br>Set up this check<br>1. Make the registered phone, email and appointment context from the Application baseline visible to the screener.<br>2. Document retry handling and legitimate forwarding, assistant, shared-calendar, connectivity and accessibility cases.<br>3. Test one benign channel issue and one genuine context/control failure.<br>Ready when: The process distinguishes an administrative or technical issue from loss of channel context or control. | Low | Developing |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-06 (+2)**<br>**Check:** Compare how the participant explains their work, role and submitted material with the written application.<br>**Score when:** *a repeatable, material shift suggests the participant does not own the submitted content and is supported by objective facts.* | STAGE BASELINE: Application baseline<br>STAGE BASELINE: Phone-screen baseline<br>BUILD ONCE: Interview baseline and continuity methods [E03] | **Delivery:** Hiring manager + HR<br>**Set up this check**<br>**1.** Use the Application and Phone-screen baselines to define the comparison fields for submitted work, role history and technical claims.<br>**2.** Apply the global materiality rule to ownership shifts and exclude accent, grammar, style and confidence; record the source statement and why any difference is material.<br>**3.** Calibrate two reviewers on a test case.<br>**Ready when:** Reviewers can distinguish normal variation from a repeatable, objective ownership shift and record the materiality rationale. | Medium | Mature |

*Table 13. Phone-screen stage: dependencies and minimum setup before each check can be used*

# STAGE 3 — INTERVIEW ROUND ONE: SET-UP SEQUENCE BEFORE USE

Before you set up this stage: the Application baseline and Phone-screen baseline are retrievable, and Approved live identity/liveness process [E02] plus Interview baseline and continuity methods [E03] are ready.

| STATUS | CHECK AND SCORE CONDITION | REQUIRED FIRST | MINIMUM TASKS TO ENABLE THIS CHECK | SETUP EFFORT | MINIMUM MATURITY |
|---|---|---|---|---|---|
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **Required baseline (0 points)**<br>**Check:** Record the approved live-video baseline, panel, date, working context and material technical statements. Use an accessible alternative where required.<br>**Record:** *The baseline must support a later trained comparison without relying on memory.* | STAGE BASELINE: Application baseline<br>STAGE BASELINE: Phone-screen baseline<br>BUILD ONCE: Approved live identity/liveness process [E02]<br>BUILD ONCE: Interview baseline and continuity methods [E03] | **Delivery:** HR + Hiring manager + DPO<br>**Set up this check**<br>**1.** Use E02 for the approved stage identity method and E03 for the Interview 1 baseline standard.<br>**2.** Record panel/date, working context and material technical statements; where the E03 Mature extension is enabled, also record the candidate-specific breadcrumb, callback-eligible statement and physical-prompt artefacts required by that standard.<br>**3.** Test retrieval by a later trained reviewer.<br>**Ready when:** A later reviewer can securely retrieve the candidate-specific Interview 1 baseline and every enabled E03 artefact without relying on memory. | Medium | Foundation |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **PHY-01 (+2)**<br>**Check:** Apply the disclosed video requirement and offer the approved alternative or reschedule route.<br>**Score when:** *the role is in scope, reasonable alternatives were offered and live verification remains unresolved.* | BUILD ONCE: Approved live identity/liveness process [E02] | **Delivery:** HR + Legal<br>Set up this check<br>1. Define which roles require live verification and disclose the requirement before the interview.<br>2. Use the E02 accessible alternative and reschedule route.<br>3. Define and test the neutral route for unresolved refusal.<br>Ready when: A test refusal follows the same non-discriminatory process and records the reason and alternatives offered. | Low | Foundation |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **PHY-02 (+3)**<br>**Check:** Where approved, use a fresh random prompt on a second device while the participant remains visible.<br>**Score when:** *the second-device image or response materially conflicts with the live person or registered channel.* | BUILD ONCE: Approved live identity/liveness process [E02]<br>BUILD ONCE: Interview baseline and continuity methods [E03]<br>BUILD ONCE: Applicant identity and contact record [E01] | **Delivery:** HR + Security + DPO<br>Set up this check<br>1. Define the second-device challenge and source of fresh random prompts within the approved E02 process.<br>2. Use E03 evidence rules for minimal capture and retrieval; apply accessibility alternatives.<br>3. Train interviewers and test benign technical failure plus a material inconsistency.<br>Ready when: Benign issues resolve correctly and a material inconsistency reaches independent review. | High | Mature |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ID-04 (+2)**<br>**Check:** Ask open, role-relevant questions about objective claims already made in the application.<br>**Score when:** *a material conflict remains after clarification and is supported by records or prior statements.* | STAGE BASELINE: Application baseline<br>STAGE BASELINE: Phone-screen baseline | **Delivery:** HR + Hiring manager<br>**Set up this check**<br>**1.** Make approved application, phone-screen and verification source material available to the panel.<br>**2.** Apply the global materiality rule to fact-based questions and record the exact source, conflict and candidate explanation.<br>**3.** Test a synthetic conflict.<br>**Ready when:** The conflict is linked to its source, the materiality rationale is recorded and subjective language is excluded. | Medium | Developing |

| | | | | | |
|---|---|---|---|---|---|
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-02 (+2)**<br>**Check:** Test only approved, non-essential details sent before the interview.<br>**Score when:** *two or more details are not known after delivery to the correct account is confirmed.* | STAGE BASELINE: Application baseline<br>BUILD ONCE: Interview baseline and continuity methods [E03] | **Delivery:** HR + Hiring manager<br>**Set up this check**<br>**1.** Use the E03-approved breadcrumb standard and selection/rotation rule; make the selected candidate-specific details plus proof of delivery available to the panel.<br>**2.** Brief the panel on the two-miss threshold, accessible alternative and one-root-cause rule.<br>**3.** Test the check before live use.<br>**Ready when:** The panel can run the check consistently without inventing breadcrumbs, scoring one forgotten detail or duplicating one root cause. | Medium | Mature |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **COM-03 (+2)**<br>**Check:** Compare the email, calendar and phone instructions used to reach the interview.<br>**Score when:** *the participant demonstrably lacks context held by the registered channels or conflicting control is observed.* | STAGE BASELINE: Application baseline<br>STAGE BASELINE: Phone-screen baseline | **Delivery:** HR<br>Set up this check<br>1. Consolidate the email, calendar and phone instructions used to reach the interview from the prior stage records.<br>2. Document legitimate forwarding, assistant and shared-calendar arrangements.<br>3. Test that the panel can reconstruct the route from records.<br>Ready when: The panel can verify channel context from evidence rather than guess who controlled a channel. | Low | Developing |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **COM-06 (+2)**<br>**Check:** Compare the participant's explanation, terminology and technical ownership with the application and phone baseline.<br>**Score when:** *a repeatable change is supported by objective content or timing evidence; grammar or accent alone is excluded.* | STAGE BASELINE: Application baseline<br>STAGE BASELINE: Phone-screen baseline<br>BUILD ONCE: Interview baseline and continuity methods [E03] | **Delivery:** Hiring manager + Security reviewer<br>**Set up this check**<br>**1.** Use the Application and Phone-screen baselines to create a comparable view of technical statements and claimed ownership.<br>**2.** Apply the global materiality rule to any ownership shift; record objective source/timing evidence and exclude grammar, accent, style and confidence.<br>**3.** Train and calibrate an independent reviewer on a test scenario.<br>**Ready when:** Reviewers agree whether the test shows normal variation or an objective ownership change and record why any difference is material. | Medium | Mature |

*Table 14. Interview-round-one stage: dependencies and minimum setup before each check can be used*

# STAGE 4 — INTERVIEW ROUND TWO: SET-UP SEQUENCE BEFORE USE

Before you set up this stage: the Interview 1 baseline is retrievable and Interview baseline and continuity methods [E03] is ready. Registered-channel control verification [E04] is required for COM-05; Approved live identity/liveness process [E02] is required for physical identity checks.

| STATUS | CHECK AND SCORE CONDITION | REQUIRED FIRST | MINIMUM TASKS TO ENABLE THIS CHECK | SETUP EFFORT | MINIMUM MATURITY |
|---|---|---|---|---|---|
| ☐ Ready<br>☐ Blocked | **Required baseline (0 points)** | EARLIER STAGE: Interview 1 baseline | **Delivery:** HR + Round-two chair<br>**Set up this check** | Medium | Mature |

| | | | | | |
|---|---|---|---|---|---|
| ☐ Out of scope | **Check:** Review the round-one baseline and choose two objective continuity points: one factual callback and one identity or channel check.<br>**Record:** *Record which points were tested and the outcome, including normal consistency.* | BUILD ONCE: Interview baseline and continuity methods [E03] | **1.** Retrieve the Interview 1 baseline and use the E03-approved callback standard to select one factual callback plus one identity/channel continuity point.<br>**2.** Nominate a different panel where possible and brief it on facts rather than suspicions.<br>**3.** Test the briefing and recording process.<br>**Ready when:** The panel can access the baseline, execute the approved method, record normal consistency and assign any unresolved observation. | | |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-04 (+2)**<br>**Check:** Restate one material, non-political point from round one inaccurately and give a fair opportunity to correct it.<br>**Score when:** *the later participant demonstrates no knowledge of the original exchange and accepts or repeats a material false attribution.* | EARLIER STAGE: Interview 1 baseline<br>BUILD ONCE: Interview baseline and continuity methods [E03] | **Delivery:** Hiring manager + Legal / HR<br>**Set up this check**<br>**1.** Use the E03-approved callback rule to select a permitted material, non-political statement whose original wording is recorded in the Interview 1 baseline.<br>**2.** Apply the E03 callback record: original statement, inaccurate restatement, fair correction opportunity and response; do not create a new callback method here.<br>**3.** Test the complete benign and mismatch sequence.<br>**Ready when:** The approved sequence is recorded and imperfect memory alone cannot create a scored signal. | Medium | Mature |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-05 (+3)**<br>**Check:** While the participant remains on camera, send separate random codes to the registered phone and email, with reasonable alternatives and retries.<br>**Score when:** *both registered channels cannot be controlled in real time after connectivity and accessibility issues are addressed.* | BUILD ONCE: Registered-channel control verification [E04]<br>EARLIER STAGE: Interview 1 baseline | **Delivery:** HR + Identity team + DPO<br>**Set up this check**<br>**1.** Use the E04 Mature simultaneous two-channel method already approved for the authoritative registered phone/email; do not redesign the random-challenge procedure in this row.<br>**2.** Apply the approved time windows, retries, accessible alternatives and minimum evidence logging.<br>**3.** Test a benign connectivity failure and a repeated loss-of-control scenario.<br>**Ready when:** Benign failure resolves while repeated inability to control both channels creates a reviewable result using the approved E04 method. | Medium | Mature |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-06 (+2)**<br>**Check:** Compare technical reasoning, claimed experience and ownership of earlier statements across the two rounds.<br>**Score when:** *a material, repeatable shift aligns with a handoff and is supported by content or timing evidence.* | STAGE BASELINE: Phone-screen baseline<br>EARLIER STAGE: Interview 1 baseline<br>BUILD ONCE: Interview baseline and continuity methods [E03] | **Delivery:** Hiring manager + Security reviewer<br>**Set up this check**<br>**1.** Create a side-by-side record of technical reasoning and earlier statements from the Phone-screen and Interview 1 baselines.<br>**2.** Apply the global materiality rule and require independent review before interpreting a handoff; record the objective content/timing evidence.<br>**3.** Test normal variation and a repeatable ownership shift.<br>**Ready when:** Reviewers distinguish style/confidence changes from an objective, repeatable shift and record the materiality rationale. | Medium | Mature |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **PHY-03 (+4)**<br>**Check:** Use the approved baseline and an independent panel to compare | BUILD ONCE: Approved live identity/liveness process [E02]<br>EARLIER STAGE: Interview 1 baseline | **Delivery:** HR + Security + Legal / DPO<br>Set up this check<br>1. Define which permitted identity/liveness evidence from E02 and the Interview 1 baseline may be compared. | High | Mature |

| | | | | | |
|---|---|---|---|---|---|
| | fundamental characteristics across rounds.<br>**Score when:** *a fundamental difference is supported by recordings or identity evidence and cannot be explained by lighting, illness or equipment.* | | 2. Apply the independent comparison method and confounder checklist: lighting, illness, equipment and synthetic-media uncertainty.<br>3. Define the disagreement/escalation route and test it.<br>Ready when: Two reviewers compare evidence rather than memory and disagreements follow the documented route. | | |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **PHY-04 (+2)**<br>**Check:** Where policy permits, repeat a simple fresh physical prompt established in round one.<br>**Score when:** *broad formation or possession is materially inconsistent enough to support a substitution hypothesis.* | BUILD ONCE: Interview baseline and continuity methods [E03]<br>EARLIER STAGE: Interview 1 baseline | **Delivery:** HR + DPO<br>**Set up this check**<br>**1.** Use the E03-approved low-risk physical-prompt standard and the candidate-specific Interview 1 prompt/outcome already recorded in the baseline.<br>**2.** Apply the permitted notice, accessible alternative and minimal-evidence rules; prohibit forensic handwriting or biometric interpretation.<br>**3.** Test that the approved prompt can be repeated consistently.<br>**Ready when:** The repeated prompt produces a neutral, repeatable observation and cannot be used as standalone proof. | High | Mature |
| *☐ Ready*<br>*☐ Blocked*<br>*☐ Out of scope* | **PHY-02 (+3)**<br>**Check:** Repeat the approved challenge with a new random prompt only when earlier evidence or risk justifies it.<br>**Score when:** *a material conflict remains after technical and accessibility explanations are excluded.* | BUILD ONCE: Approved live identity/liveness process [E02]<br>EARLIER CHECK: Interview 1 PHY-02 method and result | **Delivery:** HR + Security<br>Set up this check<br>1. Retrieve the approved Interview 1 PHY-02 method and prior result.<br>2. Define when a repeat is justified and require a fresh random prompt.<br>3. Link the repeat to the original root-cause group and test deduplication.<br>Ready when: A repeat can be run without scoring the same underlying inconsistency twice. | High | Mature |

*Table 15. Interview-round-two stage: dependencies and minimum setup before each check can be used*

# STAGE 5 — ONBOARDING: SET-UP SEQUENCE BEFORE USE

Before you set up this stage: the Application baseline and Interview 1 baseline are retrievable, and Approved live identity/liveness process [E02], Equipment delivery and device custody [E05] and HR, payroll, payment and supplier continuity [E06] are ready. Registered-channel control verification [E04] is required for COM-05. New-hire security context, access binding and telemetry [E07] is required for account, endpoint or VDI binding before first login.

| STATUS | CHECK AND SCORE CONDITION | REQUIRED FIRST | MINIMUM TASKS TO ENABLE THIS CHECK | SETUP EFFORT | MINIMUM MATURITY |
|---|---|---|---|---|---|
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **Required baseline (0 points)**<br>**Check:** Confirm the approved identity result, equipment recipient where applicable, managed endpoint or assigned VDI, corporate account, supplier record, payment owner and enrolled authentication factor/device | STAGE BASELINE: Application baseline<br>EARLIER STAGE: Interview 1 baseline<br>BUILD ONCE: Approved live identity/liveness process [E02] | **Delivery:** HR + IT + Finance + Procurement<br>Set up this check<br>1. Retrieve the candidate identity/interview evidence, the E05 delivery record where physical equipment is issued, the E06 supplier/payment records and the new-hire account/endpoint-or-VDI binding.<br>2. Create one onboarding-continuity record joining verified person, identity result, equipment recipient where applicable, managed endpoint or VDI, corporate account, enrolled authentication factor/device where supported, supplier and payment owner. | High | Developing |

| | | | | | |
|---|---|---|---|---|---|
| | where supported refer to the same authorised person or entity.<br>**Record:** *Do not release in-scope access until unresolved mismatches have an approved decision.* | BUILD ONCE: Equipment delivery and device custody [E05] - physical equipment only<br>BUILD ONCE: HR, payroll, payment and supplier continuity [E06]<br>BUILD ONCE: New-hire security context, access binding and telemetry [E07] | 3. Make unresolved mismatches an access-release gate and test a synthetic mismatch.<br>Ready when: A mismatch pauses in-scope access and creates an auditable decision rather than an informal exception. | | |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ID-07 (+3)**<br>**Check:** Verify the delivery address and named collector; route redirects, forwarding services and third-party collection through formal approval.<br>**Score when:** *the device is redirected, collected by an unexplained third party or identity proof conflicts with the hire.* | STAGE BASELINE: Application baseline<br>BUILD ONCE: Equipment delivery and device custody [E05] | **Delivery:** IT Logistics + HR<br>**Set up this check**<br>**1.** Use the canonical person/address fields from the Application baseline and the E05 record of the approved delivery destination, named recipient and chain of custody.<br>**2.** Apply formal approval for redirects, forwarding services, third-party collection and address changes.<br>**3.** Test a redirect and retrieve the complete delivery/custody record.<br>**Ready when:** A redirect creates a formal exception, the approved destination/recipient are evidenced and nothing can be approved through an untracked email. | Medium | Foundation |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **PHY-05 (+5)**<br>**Check:** Compare the approved authoritative onboarding identity/liveness result with the Interview 1 live-person baseline.<br>**Score when:** *an approved identity process identifies a material mismatch that remains unresolved.* | BUILD ONCE: Approved live identity/liveness process [E02]<br>BUILD ONCE: Interview baseline and continuity methods [E03]<br>EARLIER STAGE: Interview 1 baseline | **Delivery:** HR + Security + Identity provider + Legal<br>**Set up this check**<br>**1.** Retrieve the E02 onboarding identity/liveness result and comparison fields already defined in the Identity/Liveness Standard; compare them with the Interview 1 baseline.<br>**2.** Use E03 evidence rules, assign the comparer and independent mismatch reviewer, and record why any difference meets the global materiality rule.<br>**3.** Make an unresolved mismatch an access-release exception and test the workflow.<br>**Ready when:** A test mismatch can be retrieved, compared, independently reviewed and resolved before access is released. | High | Developing |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ADM-02 (+2)**<br>**Check:** Compare verified name, address and payment ownership across HR and payroll records.<br>**Score when:** *an objective record conflict remains unresolved; lack of benefits knowledge is not scored.* | BUILD ONCE: HR, payroll, payment and supplier continuity [E06]<br>EARLIER STAGE: Onboarding baseline | **Delivery:** HR + Finance<br>Set up this check<br>1. Use the E06 authoritative identifier and fields to compare the Onboarding baseline with payroll.<br>2. Apply the second-channel correction workflow and restricted access to payroll, tax and payment evidence.<br>3. Test a seeded name, address or payment mismatch.<br>Ready when: The mismatch creates a verification task and is not scored from benefits unfamiliarity. | Medium | Developing |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **ADM-03 (+4)**<br>**Check:** Require the provider to evidence the named worker and disclose any proposed substitution before onboarding. | BUILD ONCE: HR, payroll, payment and supplier continuity [E06] | **Delivery:** Procurement + HR + Legal<br>**Set up this check**<br>**1.** Use the E06 Supplier Verification Record plus the named-worker, substitution, subcontractor-disclosure and incident-notification requirements. | High | Developing |

| | | | | | |
|---|---|---|---|---|---|
| | **Score when:** *the provider cannot evidence identity continuity or a worker change occurred without approval.* | | **2.** Define the supplier evidence required before onboarding and the approval route for any substitution.<br>**3.** Test an attempted worker or subcontractor substitution.<br>**Ready when:** The independently verified provider cannot substitute a worker or add an undisclosed subcontractor without review. | | |
| ☐ Ready<br>☐ Blocked<br>☐ Out of scope | **COM-05 (+3)**<br>**Check:** Before releasing sensitive access, verify real-time control of the registered phone and email where policy requires it.<br>**Score when:** *both channels cannot be controlled after reasonable alternatives and retries.* | BUILD ONCE: Registered-channel control verification [E04]<br>EARLIER STAGE: Onboarding baseline | **Delivery:** HR + Identity team<br>Set up this check<br>1. Reuse the E04 real-time registered-channel control method before sensitive access is released.<br>2. Apply the approved retries, accessible alternatives and minimum evidence logging.<br>3. Make successful verification or an approved exception an access-release gate and test it.<br>Ready when: The test succeeds through both registered channels or follows the documented exception and review route. | Medium | Mature |

*Table 16. Onboarding stage: dependencies and minimum setup before each check can be used*

# STAGE 6 — FIRST 90 DAYS: SET-UP SEQUENCE BEFORE USE

Before you set up this stage: the Interview 1 baseline and Onboarding baseline are retrievable, and Equipment delivery and device custody [E05] plus New-hire security context, access binding and telemetry [E07] are ready. Approved live identity/liveness process [E02] is required for PHY-06. Where no physical equipment is issued, the equipment-delivery capability may be formally Out of scope; the assigned VDI/session context is carried by the new-hire security capability.

Additional dependency checks: Where BYOD accesses VDI, apply the E07 visibility gate; endpoint-dependent rows without equivalent evidence remain Blocked or formally Out of scope. At Developing and above, Registered-channel control verification [E04] must be Ready before first-90-day MFA reset/re-enrolment or account-recovery controls are marked Ready.

| STATUS | CHECK AND SCORE CONDITION | REQUIRED FIRST | MINIMUM TASKS TO ENABLE THIS CHECK | SETUP EFFORT | MINIMUM MATURITY |
|---|---|---|---|---|---|
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **Required baseline (0 points)**<br>**Check:** Before first login, record the new-hire work/access baseline (role, team, manager, approved systems/repositories, initial entitlements, expected task/data scope, authorised destinations and exceptions). Then complete a policy-compliant live re-verification in weeks two or three and confirm monitoring plus 30/60/90-day access reviews are active.<br>**Record:** Record the baseline and completion even when no concern exists; approved changes must remain auditable. | EARLIER STAGE: Onboarding baseline<br>BUILD ONCE: Equipment delivery and device custody [E05] - physical equipment only<br>BUILD ONCE: New-hire security context, access binding and telemetry [E07] | **Delivery:** Line manager + IAM + SOC<br>**Set up this check**<br>**1.** Use E07 before first login to create the candidate-specific work/access baseline and place the starter in the first-90-days security context.<br>**2.** Confirm the E05 user/device mapping and Onboarding baseline are available, then schedule week-two/week-three re-verification plus 30/60/90-day access reviews.<br>**3.** Test one synthetic hire from baseline creation through every required queue and one approved access/task change.<br>**Ready when:** The work/access baseline is retrievable by MIS-02/MIS-03, the hire appears in each required queue, approved changes are auditable, missed tasks alert the owner and completion is measurable. | High | Foundation → Developing |

| | | | | | |
|---|---|---|---|---|---|
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **PHY-06 (+5)**<br>**Check:** Compare the live person and device possession with the permitted hiring baseline.<br>**Score when:** a material mismatch remains and an innocent explanation is not established. | BUILD ONCE: Approved live identity/liveness process [E02]<br>BUILD ONCE: Interview baseline and continuity methods [E03]<br>EARLIER STAGE: Interview 1 baseline<br>BUILD ONCE: Equipment delivery and device custody [E05]<br>EARLIER STAGE: Onboarding baseline | **Delivery:** Line manager + HR + Security<br>**Set up this check**<br>**1.** Use the comparison fields already defined by E02/E03 for Interview 1 and onboarding, then add the E05 device-possession record; do not create a new comparison standard in this row.<br>**2.** Create the live re-verification script and immediate route to correlate a mismatch with endpoint evidence.<br>**3.** Test a mock mismatch.<br>**Ready when:** The mismatch links to the same security case, the materiality rationale is recorded and the documented review route is triggered. | Medium | Foundation |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **DEV-01 (+5)**<br>**Check:** Alert on approved-list violations, including failed or blocked installations, on newly issued devices.<br>**Score when:** the tool is outside the approved support stack and no authorised ticket explains it. | BUILD ONCE: Equipment delivery and device custody [E05]<br>BUILD ONCE: New-hire security context, access binding and telemetry [E07] | **Delivery:** Endpoint Engineering + SOC<br>**Set up this check**<br>**1.** Create and maintain the approved RMM/remote-support allow-list and authoritative support-ticket source.<br>**2.** Confirm the E07 telemetry map provides installation, execution, failed-installation, process, service and network evidence with new-hire join keys; close any mapped visibility gap before marking Ready.<br>**3.** Create the alert and test an approved tool plus a blocked-and-successful RMM chain.<br>**Ready when:** Approved support is suppressed and the simulated RMM chain creates one contextualised case using the mapped data. | High | Foundation |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **DEV-02 (+4)**<br>**Check:** Review software and configuration capable of hidden control or tunnelling.<br>**Score when:** the capability is not business-approved after developer and support exceptions are checked. | BUILD ONCE: New-hire security context, access binding and telemetry [E07] | **Delivery:** Endpoint + Network Engineering + SOC<br>**Set up this check**<br>**1.** Inventory tunnels, remote desktop tools, browser remote-control extensions and virtual cameras and define approved developer/support exceptions.<br>**2.** Use the E07 telemetry map for signer, command-line, parent-process and destination evidence with new-hire context; do not create an unmapped data dependency here.<br>**3.** Test approved and unapproved examples.<br>**Ready when:** Approved use is excluded and an unapproved capability generates a contextualised alert from mapped data. | High | Developing |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **DEV-03 (+5)**<br>**Check:** Correlate USB, network-access-control, switch, DHCP, asset and physical-support data.<br>**Score when:** evidence supports unauthorised remote hardware even though endpoint software may be absent. | BUILD ONCE: Equipment delivery and device custody [E05]<br>BUILD ONCE: New-hire security context, access binding and telemetry [E07] | **Delivery:** Network + Endpoint Engineering + IT / Physical Support<br>**Set up this check**<br>**1.** Confirm the E07 Advanced telemetry map contains retained NAC, switch, DHCP, USB, asset and physical-support sources tied to the E05 device record.<br>**2.** Join the mapped data and define the representative IP-KVM/remote-hardware pattern.<br>**3.** Build and run a lab scenario.<br>**Ready when:** The lab event creates a high-fidelity case even when endpoint software telemetry is absent. | Very high | Advanced |
| ☐ *Ready*<br>☐ *Blocked* | **DEV-04 (+3)** | BUILD ONCE: Applicant identity and contact record [E01] | **Delivery:** Identity team + SOC + HR<br>Set up this check | High | Developing |

| | | | | | |
|---|---|---|---|---|---|
| ☐ *Out of scope* | **Check:** Compare identity-provider sessions, managed endpoint or VDI data, MFA/authentication-factor telemetry, factor reset/re-enrolment or account-recovery events and registered working context.<br>**Score when:** events conflict with the expected access path or indicate multiple operators after VPN, travel, VDI and mobile use are excluded. | BUILD ONCE: New-hire security context, access binding and telemetry [E07]<br>BUILD ONCE: Registered-channel control verification [E04]<br>EARLIER STAGE: Onboarding baseline | 1. Use New-hire security context, access binding and telemetry [E07] to baseline the managed endpoint or assigned VDI and enrolled factor/device against the registered working context from Applicant identity and contact record [E01]/Onboarding; use Registered-channel control verification [E04] for first-90-day reset, re-enrolment or account recovery.<br>2. Document legitimate VPN, travel, VDI and mobile exceptions; do not treat a successful OTP/MFA event as proof that the same person controls the session.<br>3. Correlate identity-provider, endpoint/VDI, authentication-factor and recovery/re-enrolment events and test a seeded mismatch, relay or factor-change scenario.[19]<br>Ready when: An endpoint/VDI-versus-factor, session-concurrency or recovery/re-enrolment mismatch creates one case with legitimate exceptions available to triage. | | |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **DEV-05 (+3)**<br>**Check:** Review managed endpoint or VDI tooling/profile activity that aggregates or synchronises identities, browsers, employers or messaging accounts.<br>**Score when:** the activity/tooling is outside role requirements and provides objective evidence of multiple identities or employers after approved testing, support and benign personal use are excluded. | BUILD ONCE: New-hire security context, access binding and telemetry [E07] | **Delivery:** Endpoint Engineering + SOC + Manager<br>**Set up this check**<br>**1.** Use the E07 telemetry map to identify visible persona-management, multi-profile/account-aggregation and personal browser-profile synchronisation activity; record any VDI/BYOD visibility gap before enabling the check.<br>**2.** Define role-based policy, allow-lists and approved testing/support or benign personal-profile exceptions; personal sign-in or synchronisation alone does not score.<br>**3.** Create and test the detection.<br>**Ready when:** Approved or benign personal use is suppressed and an unapproved multi-identity condition identifies the affected identities and services. | High | Mature |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **MIS-01 (+4)**<br>**Check:** Triage controlled decoy interactions using the documented benign path.<br>**Score when:** the decoy is used in a sequence or destination inconsistent with legitimate work. | UNIVERSAL: Live-use prerequisites<br>BUILD ONCE: New-hire security context, access binding and telemetry [E07] | **Delivery:** Security + DPO + Legal<br>Set up this check<br>1. Define the controlled canary file or honeypot credential and document its benign path.<br>2. Complete monitoring notice, evidence retention and response routing within the approved live-use guardrails.<br>3. Test accidental interaction and an adversarial sequence.<br>Ready when: Accidental use resolves without escalation while adversarial use creates reviewable evidence. | High | Mature |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **MIS-02 (+5)**<br>**Check:** Correlate repository, DLP, cloud, USB and web activity with the assigned task.<br>**Score when:** volume, destination and timing exceed legitimate development, build, backup or migration activity. | BUILD ONCE: New-hire security context, access binding and telemetry [E07]<br>STAGE BASELINE: First-90-days work/access baseline | **Delivery:** SOC + Data Security + Engineering<br>**Set up this check**<br>**1.** Use the First-90-days work/access baseline to confirm legitimate repositories, build/backup/migration activity, task/data scope and authorised destinations for this starter; manager/Engineering approve any exceptions.<br>**2.** Use the E07 telemetry map to join repository, DLP, cloud, USB and web evidence to the starter and define the active-exfiltration response.<br>**3.** Test a bulk clone plus controlled transfer.<br>**Ready when:** The test creates one joined case while activity inside the approved work/access baseline is excluded. | High | Mature |

| | | | | | |
|---|---|---|---|---|---|
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **MIS-03 (+3)**<br>**Check:** Review repeated access to secrets, systems or data unrelated to the assigned role.<br>**Score when:** the access remains unexplained after entitlement and manager expectations are checked. | BUILD ONCE: New-hire security context, access binding and telemetry [E07]<br>STAGE BASELINE: First-90-days work/access baseline | **Delivery:** IAM + Line manager + SOC<br>**Set up this check**<br>**1.** Use the First-90-days work/access baseline as the role-access map; confirm least privilege and document approved entitlement changes or temporary exceptions.<br>**2.** Use the E07 telemetry map to retain secrets/system audit evidence and define manager validation plus entitlement-removal workflow.<br>**3.** Test an access event outside task scope.<br>**Ready when:** The event reaches entitlement review, approved exceptions are visible and access can be reduced regardless of attribution. | Medium | Mature |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **MIS-04 (+3)**<br>**Check:** Use objective managed-device, collaboration and session evidence to test whether several people or employers are involved.<br>**Score when:** evidence indicates other employer systems or multiple operators and cannot be explained by approved work. | BUILD ONCE: New-hire security context, access binding and telemetry [E07]<br>EARLIER STAGE: Onboarding baseline | **Delivery:** Detection Engineering + Insider Risk + HR<br>Set up this check<br>1. Select the managed-device, collaboration and session data used to test operator rotation and define approved shift/shared-infrastructure baselines.<br>2. Complete privacy review and define a representative multi-operator scenario.<br>3. Build and test the analytics.<br>Ready when: Test data separates legitimate shifts/shared infrastructure from unexplained identity rotation. | Very high | Advanced |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **ADM-01 (+2)**<br>**Check:** Verify changes through the established channel and correlate the session or device used to make them.<br>**Score when:** the change is repeated, unusual or coincides with conflicting identity, device or session evidence. | BUILD ONCE: Registered-channel control verification [E04]<br>BUILD ONCE: HR, payroll, payment and supplier continuity [E06]<br>EARLIER STAGE: Onboarding baseline | **Delivery:** HR + Finance + Identity team<br>Set up this check<br>1. Define which early bank, payment, address and contact changes require known-channel verification.<br>2. Use E04/E06 to verify the change and capture the session or device used to request it.<br>3. Test an early administrative change.<br>Ready when: The change creates a verification task and can be joined to identity or device evidence. | Medium | Developing |
| ☐ *Ready*<br>☐ *Blocked*<br>☐ *Out of scope* | **ADM-02 (+2)**<br>**Check:** Compare payroll, tax, address and payment ownership with verified onboarding records.<br>**Score when:** an objective conflict remains unresolved after correction routes are offered. | BUILD ONCE: HR, payroll, payment and supplier continuity [E06]<br>EARLIER STAGE: Onboarding baseline | **Delivery:** HR + Finance<br>Set up this check<br>1. Use the E06 authoritative fields from the Onboarding baseline for payroll, tax, address and payment ownership.<br>2. Configure reconciliation, correction routes and restricted access to the resulting evidence.<br>3. Test a seeded conflict.<br>Ready when: The conflict is assigned, explained and resolved or remains open with a named owner. | Medium | Developing |

*Table 17. First-90-days stage: dependencies and minimum setup before each check can be used*

**Setup status and case result are different.** Use Ready, Blocked or Out of scope here; use N/A only in live case forms. **Go-live gate:** every in-scope row at or below the current maturity must be Ready or formally Out of scope; none may be Blocked. Critical overrides still apply at any maturity.

# CASE SHEET

| CASE DETAILS — complete once | | | | | |
|---|---|---|---|---|---|
| **Candidate / employee** | | **Role / business unit** | | **Case owner** | |
| **Engagement type** | Employee / contractor / agency / other | **Date opened** | | **Retention date** | |
| **Scope / rationale** | | | | **Case reference** | |
| **CUMULATIVE STAGE TRACKER — summary only; evidence stays in the stage form** | | | | | |
| **Stage** | **Status** | **Stage score** | **Cumulative** | **Domains** | **Reviewer / next action** |
| **Application** | Open / complete / N/A | | | | |
| **Phone screen** | Open / complete / N/A | | | | |
| **Interview one** | Open / complete / N/A | | | | |
| **Interview two** | Open / complete / N/A | | | | |
| **Onboarding** | Open / complete / N/A | | | | |
| **First 90 days** | Open / complete / N/A | | | | |
| **CURRENT DECISION — update after each stage** | | | | | |
| **Tier** | Baseline / Elevated / High / Critical | **Override?** | Yes / No | **Second reviewer?** | Yes / No |
| **Open signal IDs** | | **Domains** | | **Stages** | |
| **Explanation / next action / owner / due date** | | | | | |
| **Decision / approval** | | **Approved by / date** | | **Retention checked?** | Yes / No |

*Table 18. Case cover and cumulative decision sheet*

Return to workbook navigation

# STAGE 1 — APPLICATION REVIEW

Owner: HR screening coordinator. Use before a phone screen is booked. Run the same baseline for every in-scope applicant. Do not score names, nationality, grammar, profile style or low rates. **Use only rows marked ready in the matching application setup table; mark all others N/A.**

| DONE | CHECK AND SCORE CONDITION | RESULT | SIGNAL / FIXED POINTS | EVIDENCE REFERENCE / BRIEF NOTE |
|---|---|---|---|---|
| ☐ | Confirm the application source, role, declared identity, contact details, proposed equipment-delivery address and, where applicable, referral/introducer/internal sponsor.<br>*Record: Record completion and route any objective discrepancy to the relevant signal below.* | COMPLETE / EXCEPTION | **Required**<br>**0** | Ref: _____<br>Note: |
| ☐ | Run the approved carrier lookup on the declared primary number where policy permits.<br>*Score when: the result is verified as VoIP. VoIP use alone is not suspicious.* | NC / EXP / OPEN / N/A | **ID-01**<br>**0 or +1** | Ref: _____<br>Note: |
| ☐ | Search the applicant tracking system across active applications and recent hires for the same phone number or email.<br>*Score when: apparently unrelated identities share the contact point and household, agency or data-entry explanations are excluded.* | NC / EXP / OPEN / N/A | **ID-02**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Compare residential and proposed delivery addresses across applicants and recent hires.<br>*Score when: the same address appears across unrelated identities with no credible relationship.* | NC / EXP / OPEN / N/A | **ID-03**<br>**0 or +4** | Ref: _____<br>Note: |
| ☐ | Compare dates, names, education and employment claims across the application and approved verification sources.<br>*Score when: a material conflict remains after the applicant has a fair opportunity to correct or explain it.* | NC / EXP / OPEN / N/A | **ID-04**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Where references occur at this stage, source the organisation or referee independently rather than using only candidate-provided details.<br>*Score when: the referee or employer cannot be validated through an independently sourced route after reasonable attempts.* | NC / EXP / OPEN / N/A | **ID-05**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Check whether an agency, referee, referral/introducer/internal sponsor, domain or contact point appears across several apparently unrelated candidates.<br>*Score when: a repeated cluster cannot be explained by an approved supplier or shared service.* | NC / EXP / OPEN / N/A | **ID-06**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Only where approved, rotate an accessible and policy-reviewed automation canary across separate communications.<br>*Score when: two or more triggers occur after mail-system artefacts and assistive-technology explanations are excluded.* | NC / EXP / OPEN / N/A | **COM-01**<br>**0 or +1** | Ref: _____<br>Note: |
| **STAGE CLOSE** | | | | |
| **Stage score**<br>_____ | **Cumulative**<br>_____ | **Domains**<br>_____ | **Open signal IDs**<br>_____ | **Status**<br>_____ |
| **Explanation / root cause / next action / owner / due date:**<br>Before booking the phone screen, record completion, any open signal IDs, the explanation obtained and the owner of the next action. | | | | |

*Table 19. Stage 1: Application review stage form*

Return to workbook navigation

# STAGE 2 — PHONE SCREEN

Owner: HR screener or hiring manager. Use this as a communication and factual-ownership baseline. Do not score accent, fluency, timezone trivia, cultural knowledge, nervousness or a single forgotten detail. **Use only rows marked ready in the matching phone-screen setup table; mark all others N/A.**

| DONE | CHECK AND SCORE CONDITION | RESULT | SIGNAL / FIXED POINTS | EVIDENCE REFERENCE / BRIEF NOTE |
|---|---|---|---|---|
| ☐ | Confirm the participant's name, role, registered phone and email, and ask them to summarise the material application in their own words.<br>*Record: Record who participated, the channels used and any explanation for differences.* | COMPLETE / EXCEPTION | **Required**<br>**0** | Ref: _____<br>Note: |
| ☐ | Revisit one or two objective education, employment or role details already supplied in the application.<br>*Score when: a material conflict remains after a clear and fair prompt; normal memory variation is not scored.* | NC / EXP / OPEN / N/A | **ID-04**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Where approved, ask about two non-essential details previously sent to the registered account.<br>*Score when: multiple details are not known after confirming the correspondence reached the correct account.* | NC / EXP / OPEN / N/A | **COM-02**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Confirm that the person can use the registered phone and email and understands the current process and appointment.<br>*Score when: objective evidence suggests different people control the channels or the participant lacks material context from registered communications.* | NC / EXP / OPEN / N/A | **COM-03**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Compare how the participant explains their work, role and submitted material with the written application.<br>*Score when: a repeatable, material shift suggests the participant does not own the submitted content and is supported by objective facts.* | NC / EXP / OPEN / N/A | **COM-06**<br>**0 or +2** | Ref: _____<br>Note: |
| **STAGE CLOSE** | | | | |
| **Stage score**<br>_____ | **Cumulative**<br>_____ | **Domains**<br>_____ | **Open signal IDs**<br>_____ | **Status**<br>_____ |
| **Explanation / root cause / next action / owner / due date:**<br>Record the stage score, domains and the exact issue—if any—that the interview panel must resolve. | | | | |

*Table 20. Stage 2: Phone screen stage form*

Return to workbook navigation

# STAGE 3 — INTERVIEW ROUND ONE

Owner: Hiring manager or interviewer. Create the live identity and working-context baseline that later stages will compare against. Use enhanced checks only where policy, notice, accessibility and maturity support them. **Use only rows marked ready in the matching interview-one setup table; mark all others N/A.**

| DONE | CHECK AND SCORE CONDITION | RESULT | SIGNAL / FIXED POINTS | EVIDENCE REFERENCE / BRIEF NOTE |
|---|---|---|---|---|
| ☐ | Record the approved live-video baseline, panel, date, working context and material technical statements. Use an accessible alternative where required.<br>*Record: The baseline must support a later trained comparison without relying on memory.* | COMPLETE / EXCEPTION | **Required**<br>**0** | Ref: _____<br>Note: |
| ☐ | Apply the disclosed video requirement and offer the approved alternative or reschedule route.<br>*Score when: the role is in scope, reasonable alternatives were offered and live verification remains unresolved.* | NC / EXP / OPEN / N/A | **PHY-01**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Where approved, use a fresh random prompt on a second device while the participant remains visible.<br>*Score when: the second-device image or response materially conflicts with the live person or registered channel.* | NC / EXP / OPEN / N/A | **PHY-02**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Ask open, role-relevant questions about objective claims already made in the application.<br>*Score when: a material conflict remains after clarification and is supported by records or prior statements.* | NC / EXP / OPEN / N/A | **ID-04**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Test only approved, non-essential details sent before the interview.<br>*Score when: two or more details are not known after delivery to the correct account is confirmed.* | NC / EXP / OPEN / N/A | **COM-02**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Compare the email, calendar and phone instructions used to reach the interview.<br>*Score when: the participant demonstrably lacks context held by the registered channels or conflicting control is observed.* | NC / EXP / OPEN / N/A | **COM-03**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Compare the participant's explanation, terminology and technical ownership with the application and phone baseline.<br>*Score when: a repeatable change is supported by objective content or timing evidence; grammar or accent alone is excluded.* | NC / EXP / OPEN / N/A | **COM-06**<br>**0 or +2** | Ref: _____<br>Note: |
| **STAGE CLOSE** | | | | |
| **Stage score**<br>_____ | **Cumulative**<br>_____ | **Domains**<br>_____ | **Open signal IDs**<br>_____ | **Status**<br>_____ |
| **Explanation / root cause / next action / owner / due date:**<br>Preserve the permitted baseline, record unresolved facts and give the round-two panel a short verification brief—not a conclusion about the person. | | | | |

*Table 21. Stage 3: Interview round one stage form*

Return to workbook navigation

# STAGE 4 — INTERVIEW ROUND TWO

Owner: Different panel where possible. Compare the same identity across time, channels and factual ownership. A normal change in lighting, clothing, equipment or confidence is not a signal by itself. **Use only rows marked ready in the matching interview-two setup table; mark all others N/A.**

| DONE | CHECK AND SCORE CONDITION | RESULT | SIGNAL / FIXED POINTS | EVIDENCE REFERENCE / BRIEF NOTE |
|---|---|---|---|---|
| ☐ | Review the round-one baseline and choose two objective continuity points: one factual callback and one identity or channel check.<br>*Record: Record which points were tested and the outcome, including normal consistency.* | COMPLETE / EXCEPTION | **Required**<br>**0** | Ref: _____<br>Note: |
| ☐ | Restate one material, non-political point from round one inaccurately and give a fair opportunity to correct it.<br>*Score when: the later participant demonstrates no knowledge of the original exchange and accepts or repeats a material false attribution.* | NC / EXP / OPEN / N/A | **COM-04**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | While the participant remains on camera, send separate random codes to the registered phone and email, with reasonable alternatives and retries.<br>*Score when: both registered channels cannot be controlled in real time after connectivity and accessibility issues are addressed.* | NC / EXP / OPEN / N/A | **COM-05**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Compare technical reasoning, claimed experience and ownership of earlier statements across the two rounds.<br>*Score when: a material, repeatable shift aligns with a handoff and is supported by content or timing evidence.* | NC / EXP / OPEN / N/A | **COM-06**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Use the approved baseline and an independent panel to compare fundamental characteristics across rounds.<br>*Score when: a fundamental difference is supported by recordings or identity evidence and cannot be explained by lighting, illness or equipment.* | NC / EXP / OPEN / N/A | **PHY-03**<br>**0 or +4** | Ref: _____<br>Note: |
| ☐ | Where policy permits, repeat a simple fresh physical prompt established in round one.<br>*Score when: broad formation or possession is materially inconsistent enough to support a substitution hypothesis.* | NC / EXP / OPEN / N/A | **PHY-04**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Repeat the approved challenge with a new random prompt only when earlier evidence or risk justifies it.<br>*Score when: a material conflict remains after technical and accessibility explanations are excluded.* | NC / EXP / OPEN / N/A | **PHY-02**<br>**0 or +3** | Ref: _____<br>Note: |
| **STAGE CLOSE** | | | | |
| **Stage score**<br>_____<br>_____ | **Cumulative**<br>_____ | **Domains**<br>_____ | **Open signal IDs**<br>_____ | **Status**<br>_____ |
| **Explanation / root cause / next action / owner / due date:**<br>Update the cumulative case sheet and corroboration gates. A high number without independent domains or stages does not create a high-concern case. | | | | |

*Table 22. Stage 4: Interview round two stage form*

Return to workbook navigation

# STAGE 5 — ONBOARDING

Owner: HR, IT and Security. Bind the verified person to the device recipient, corporate account, supplier record and payment identity before privileged or production access is released. **Use only rows marked ready in the matching onboarding setup table; mark all others N/A.**

| DONE | CHECK AND SCORE CONDITION | RESULT | SIGNAL / FIXED POINTS | EVIDENCE REFERENCE / BRIEF NOTE |
|---|---|---|---|---|
| ☐ | Confirm the approved identity result, equipment recipient where applicable, managed endpoint or assigned VDI, corporate account, supplier record, payment owner and enrolled authentication factor/device where supported refer to the same authorised person or entity.<br>*Record: Do not release in-scope access until unresolved mismatches have an approved decision.* | COMPLETE / EXCEPTION | **Required**<br>**0** | Ref: _____<br>Note: |
| ☐ | Verify the delivery address and named collector; route redirects, forwarding services and third-party collection through formal approval.<br>*Score when: the device is redirected, collected by an unexplained third party or identity proof conflicts with the hire.* | NC / EXP / OPEN / N/A | **ID-07**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Compare the approved authoritative onboarding identity/liveness result with the Interview 1 live-person baseline.<br>*Score when: an approved identity process identifies a material mismatch that remains unresolved.* | NC / EXP / OPEN / N/A | **PHY-05**<br>**0 or +5** | Ref: _____<br>Note: |
| ☐ | Compare verified name, address and payment ownership across HR and payroll records.<br>*Score when: an objective record conflict remains unresolved; lack of benefits knowledge is not scored.* | NC / EXP / OPEN / N/A | **ADM-02**<br>**0 or +2** | Ref: _____<br>Note: |
| ☐ | Require the provider to evidence the named worker and disclose any proposed substitution before onboarding.<br>*Score when: the provider cannot evidence identity continuity or a worker change occurred without approval.* | NC / EXP / OPEN / N/A | **ADM-03**<br>**0 or +4** | Ref: _____<br>Note: |
| ☐ | Before releasing sensitive access, verify real-time control of the registered phone and email where policy requires it.<br>*Score when: both channels cannot be controlled after reasonable alternatives and retries.* | NC / EXP / OPEN / N/A | **COM-05**<br>**0 or +3** | Ref: _____<br>Note: |
| **STAGE CLOSE** | | | | |
| **Stage score**<br>_____<br>_____<br>__ | **Cumulative**<br>_____ | **Domains**<br>_____ | **Open signal IDs**<br>_____ | **Status**<br>_____ |
| **Explanation / root cause / next action / owner / due date:**<br>The person, device recipient, account and payment destination are either bound together or a named decision owner has paused and escalated the exception. | | | | |

*Table 23. Stage 5: Onboarding stage form*

Return to workbook navigation

# STAGE 6 — FIRST 90 DAYS

Owner: Line manager, SOC, insider risk and Finance. Use only checks supported by the organisation's maturity and available telemetry. High use of artificial intelligence or translation services alone is not suspicious. **Use only rows marked ready in the matching first-90-days setup table; mark all others N/A.**

| DONE | CHECK AND SCORE CONDITION | RESULT | SIGNAL / FIXED POINTS | EVIDENCE REFERENCE / BRIEF NOTE |
|---|---|---|---|---|
| ☐ | Confirm the new-hire work/access baseline was recorded before first login: role, team, manager, approved systems/repositories, initial entitlements, expected task/data scope, authorised destinations and exceptions. Complete the policy-compliant live re-verification in weeks two or three and confirm monitoring plus 30/60/90-day access reviews are active.<br>**Record:** Record completion and approved changes even when no concern exists. | COMPLETE / EXCEPTION | **Required**<br>**0** | Ref: _____<br>Note: |
| ☐ | Compare the live person and device possession with the permitted hiring baseline.<br>*Score when: a material mismatch remains and an innocent explanation is not established.* | NC / EXP / OPEN / N/A | **PHY-06**<br>**0 or +5** | Ref: _____<br>Note: |
| ☐ | Alert on approved-list violations, including failed or blocked installations, on newly issued devices.<br>*Score when: the tool is outside the approved support stack and no authorised ticket explains it.* | NC / EXP / OPEN / N/A | **DEV-01**<br>**0 or +5** | Ref: _____<br>Note: |
| ☐ | Review software and configuration capable of hidden control or tunnelling.<br>*Score when: the capability is not business-approved after developer and support exceptions are checked.* | NC / EXP / OPEN / N/A | **DEV-02**<br>**0 or +4** | Ref: _____<br>Note: |
| ☐ | Correlate USB, network-access-control, switch, DHCP, asset and physical-support data.<br>*Score when: evidence supports unauthorised remote hardware even though endpoint software may be absent.* | NC / EXP / OPEN / N/A | **DEV-03**<br>**0 or +5** | Ref: _____<br>Note: |
| ☐ | Compare identity-provider sessions, managed endpoint or VDI data, MFA/authentication-factor telemetry, factor reset/re-enrolment or account-recovery events and registered working context. | NC / EXP / OPEN / N/A | **DEV-04**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Review managed endpoint or VDI tooling/profile activity that aggregates or synchronises identities, browsers, employers or messaging accounts.<br>*Score when: the activity/tooling is outside role requirements and provides objective evidence of multiple identities or employers after approved testing, support and benign personal use are excluded.* | NC / EXP / OPEN / N/A | **DEV-05**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Triage controlled decoy interactions using the documented benign path.<br>*Score when: the decoy is used in a sequence or destination inconsistent with legitimate work.* | NC / EXP / OPEN / N/A | **MIS-01**<br>**0 or +4** | Ref: _____<br>Note: |
| ☐ | Correlate repository, DLP, cloud, USB and web activity with the assigned task.<br>*Score when: volume, destination and timing exceed legitimate development, build, backup or migration activity.* | NC / EXP / OPEN / N/A | **MIS-02**<br>**0 or +5** | Ref: _____<br>Note: |
| ☐ | Review repeated access to secrets, systems or data unrelated to the assigned role.<br>*Score when: the access remains unexplained after entitlement and manager expectations are checked.* | NC / EXP / OPEN / N/A | **MIS-03**<br>**0 or +3** | Ref: _____<br>Note: |
| ☐ | Use objective managed-device, collaboration and session evidence to test whether several people or employers are involved.<br>*Score when: evidence indicates other employer systems or multiple operators and cannot be explained by approved work.* | NC / EXP / OPEN / N/A | **MIS-04**<br>**0 or +3** | Ref: _____<br>Note: |

| DONE | CHECK AND SCORE CONDITION | RESULT | SIGNAL / FIXED POINTS | EVIDENCE REFERENCE / BRIEF NOTE |
|---|---|---|---|---|
| ☐ | Verify changes through the established channel and correlate the session or device used to make them.<br>*Score when: the change is repeated, unusual or coincides with conflicting identity, device or session evidence.* | NC / EXP / OPEN / N/A | **ADM-01**<br>**0 or +2** | Ref: _____<br>Note: |
| | | | | |
| ☐ | Compare payroll, tax, address and payment ownership with verified onboarding records.<br>*Score when: an objective conflict remains unresolved after correction routes are offered.* | NC / EXP / OPEN / N/A | **ADM-02**<br>**0 or +2** | Ref: _____<br>Note: |
| **STAGE CLOSE** | | | | |
| **Stage score**<br>_____<br>_____ | **Cumulative**<br>_____ | **Domains**<br>_____ | **Open signal IDs**<br>_____ | **Status**<br>_____ |
| **Explanation / root cause / next action / owner / due date:**<br>Update the cumulative case sheet, access review and decision. Use a critical override for verified substitution, active exfiltration or unauthorised remote control rather than waiting for the total score. | | | | |

*Table 24. Stage 6: First 90 days stage form*

Return to workbook navigation

# ESCALATION AND CORROBORATION REVIEW

Use this sheet only when the cumulative score reaches 5, a five-point signal is selected, a critical override is suspected or a second reviewer is required. Do not repeat full evidence: refer to the open signal IDs and stage-form references.

| *REVIEW QUESTION* | FINDING / EVIDENCE REFERENCE | DECISION | OWNER / DATE |
|---|---|---|---|
| ***Which open signal IDs remain after explanations?*** | | Open / resolved | |
| ***Which observations share one root cause?*** | | Count once / separate | |
| ***Which independent evidence domains are represented?*** | | Number: ____ | |
| ***Which independent lifecycle stages are represented?*** | | Number: ____ | |
| ***Is there verified identity substitution?*** | | Yes / No | |
| ***Is there active or confirmed exfiltration?*** | | Yes / No | |
| ***Is there unauthorised remote control?*** | | Yes / No | |

| | | | |
|---|---|---|---|
| ***Which response tier applies after the gate?*** | | Baseline / Elevated / High concern / Critical | |
| ***What action is authorised?*** | | Verify / investigate / contain / close | |
| ***Who approved the action and evidence retention?*** | | Approved / returned | |

*Table 25. Escalation, corroboration and approval review*

| TIER | INDICATIVE STARTING POINT | REQUIRED GATE | ACTION |
|---|---|---|---|
| **Baseline** | 0–4 | No unresolved strong signal | Continue standard controls and resolve open observations. |
| **Elevated** | 5–8 | At least two independent domains | Use proportionate enhanced verification and notify Security. |
| **High concern** | 9–12 | Evidence from at least two stages and independent review | Notify the Programme Owner; intensify review and consider targeted open-source intelligence where justified. |
| **Critical** | 13+ | At least one strong signal plus cross-domain corroboration | Convene Security, HR, Legal and Compliance; assess access, containment and reporting. |
| **Critical override** | Any score | Verified substitution, active exfiltration or unauthorised remote control | Begin immediate security and insider-risk review. |

*Table 26. Response-tier quick reference*

**Coverage check.** The response-tier bands assume the enabled scorecard provides meaningful opportunities to observe independent domains. If maturity, policy, telemetry gaps or deliberate exclusions materially change the checks in use, re-evaluate the bands before live scoring using synthetic or retrospective cases and reviewer agreement. Do not lower thresholds mechanically to compensate for missing controls. Document the approved rationale. Critical overrides remain unchanged.

# WORKED EXAMPLES: WHAT THE SCORE CHANGES

Use the examples to teach reviewers that the number is never the entire decision. The domain, stage, root cause, explanation and presence of active harm determine the next step.

| *SCENARIO* | RECORDED FACTS | GATE | REQUIRED ACTION |
|---|---|---|---|
| *A. Baseline observation* | Verified VoIP number (+1). One forgotten breadcrumb is recorded but not scored. | One weak signal in one domain; no strong signal. | Resolve the open observation and continue standard controls. Do not add intrusive checks. |
| *B. Elevated verification* | Phone or email reused across unrelated applicants (+3) plus a material cross-channel inconsistency (+2). | Score 5 across identity and communication domains. | Notify Security and run proportionate verification, such as independent contact and simultaneous channel control. No accusation or automatic rejection. |
| *C. High concern / override* | Unrelated identities share a delivery address (+4) and an unapproved RMM installation is attempted (+5). | Score 9 across application and post-hire stages; second reviewer required. | Begin coordinated review. If remote control is active, preserve evidence and assess containment immediately rather than waiting for more points. |

| | | |
|---|---|---|
| | Active remote control is a critical override. | |

*Table 27. Worked scoring examples for baseline, elevated and critical decisions*

# ROOT-CAUSE AND DEDUPLICATION EXAMPLES

Count one underlying cause once. A repeated observation becomes a new score only when it is supported by genuinely independent evidence.

| OBSERVED PATTERN | TREAT AS | REASON |
|---|---|---|
| *Poor connectivity causes degraded video, delayed codes and broken audio in one session.* | One root cause | Do not turn one connectivity problem into three separate signals. |
| *The same channel-control failure appears in interview two and onboarding.* | Usually one root cause | Link the later observation to the original signal unless new independent evidence exists. |
| *An unexplained reused delivery address is followed by unapproved RMM activity.* | Separate domains | Identity/delivery and device-control evidence are independent and may corroborate each other. |

*Table 28. Examples of root-cause grouping and corroboration*

# SIGNAL-TO-STAGE MAP

Use this map when reviewing a case across stages. The current-stage form remains the primary operating view.

| STAGE | REQUIRED BASELINE | SIGNALS AVAILABLE AT THIS STAGE | MAIN DOMAINS |
|---|---|---|---|
| Application | Identity, contact and delivery details | ID-01–ID-06; COM-01 where approved | Identity; communication |
| Phone screen | Registered channels and factual ownership | ID-04; COM-02, COM-03, COM-06 | Identity; communication |
| Interview one | Live identity and working-context baseline | PHY-01, PHY-02; ID-04; COM-02, COM-03, COM-06 | Physical; identity; communication |
| Interview two | Cross-round continuity and channel control | COM-04, COM-05, COM-06; PHY-02, PHY-03, PHY-04 | Communication; physical |
| Onboarding | Person, recipient, account, supplier and payment bound together | ID-07; PHY-05; ADM-02, ADM-03; COM-05 | Identity; physical; administration |
| First 90 days | Re-verification, access review and telemetry checks | PHY-06; DEV-01–DEV-05; MIS-01–MIS-04; ADM-01, ADM-02 | Physical; device; mission; administration |

*Table 29. Signals expected at each lifecycle stage*

# SIGNAL GUARDRAIL INDEX

Reference only — do not complete these tables. The setup rows and writable stage forms are authoritative for definitions and scoring conditions; use this index only to confirm the primary stage, key guardrail and next action.

# IDENTITY AND INFRASTRUCTURE — APPLICATION, ONBOARDING AND CROSS-CASE ANALYSIS

| SIGNAL | PTS | PRIMARY STAGE | KEY GUARDRAIL | NEXT ACTION |
|---|---|---|---|---|
| *ID-01* | +1 | Application | VoIP is common legitimate usage; never act on it alone. | Confirm control through another approved channel. |
| *ID-02* | +3 | Application | Exclude household, agency and data-entry explanations. | Review linked applicants and recent hires. |
| *ID-03* | +4 | Application | Shared housing and supplier addresses can be legitimate. | Verify recipient, delivery history and equipment count. |
| *ID-04* | +2 | Application / phone / interviews | Use source-linked materiality and give a fair correction/explanation route. | Independently verify any unresolved material conflict. |
| *ID-05* | +3 | Application | A failed candidate-supplied email is not enough. | Use switchboard, corporate domain or trusted provider. |
| *ID-06* | +3 | Application / cross-case | Referral, sponsorship or supplier reuse is not suspicious by itself. | Review stated relationships and approved supplier records. |
| *ID-07* | +3 | Onboarding | Redirects or third-party collection require formal approval; do not infer intent from logistics alone. | Pause shipment/access and verify through the established channel. |

*Table 30. Signal guardrails: identity and infrastructure*

## COMMUNICATION CONTINUITY — PHONE SCREEN AND INTERVIEWS

| SIGNAL | PTS | PRIMARY STAGE | KEY GUARDRAIL | NEXT ACTION |
|---|---|---|---|---|
| *COM-01* | +1 | Application | Automation, screen readers and legitimate AI can trigger it; one result never scores. | Exclude mail/assistive artefacts and require human review. |
| *COM-02* | +2 | Phone screen / interview one | One forgotten detail never scores; prove delivery to the correct account. | Resolve delivery/recall issues before scoring. |
| *COM-03* | +2 | Phone screen / interview one | Forwarding, assistants, shared calendars, accessibility and device issues can explain differences. | Reconstruct the channel route from records. |
| *COM-04* | +2 | Interview two | Memory is imperfect; use a material, non-political, source-recorded detail. | Corroborate the mismatch elsewhere before escalation. |
| *COM-05* | +3 | Interview two / onboarding | Tests channel control only; codes and approvals can be relayed. | Use DEV-04 for corporate session/device continuity. |
| *COM-06* | +2 | Phone / interviews | Grammar, accent, style and confidence are excluded. | Seek repeatable objective content or timing evidence. |

*Table 31. Signal guardrails: communication continuity*

## PHYSICAL IDENTITY CONTINUITY — INTERVIEWS, ONBOARDING AND FIRST 90 DAYS

| SIGNAL | PTS | PRIMARY STAGE | KEY GUARDRAIL | NEXT ACTION |
|---|---|---|---|---|
| PHY-01 | +2 | Interview one | Safety, disability, religion, privacy and connectivity may justify alternatives. | Use the neutral unresolved/refusal route. |
| PHY-02 | +3 | Interview one / two | A static image or one prompt is not proof; use fresh prompts and minimal evidence. | Route material inconsistency to independent review. |
| PHY-03 | +4 | Interview two | Lighting, illness, equipment and synthetic-media artefacts can mislead. | Require independent evidence-based comparison. |
| PHY-04 | +2 | Interview two | Not forensic handwriting or biometric analysis; it is supporting continuity evidence only. | Treat as a lead and corroborate. |
| PHY-05 | +5 | Onboarding | Use only the approved identity/liveness process and materiality rule. | Pause access and escalate unresolved mismatch to HR, Security and Legal. |
| *PHY-06* | +5 | First 90 days | Consider innocent device/working-context explanations before scoring. | Correlate a mismatch with endpoint/device evidence immediately. |

*Table 32. Signal guardrails: physical identity continuity*

## DEVICE AND ACCESS CONTINUITY — ONBOARDING AND FIRST 90 DAYS

| SIGNAL | PTS | PRIMARY STAGE | KEY GUARDRAIL | NEXT ACTION |
|---|---|---|---|---|
| *DEV-01* | +5 | First 90 days | Exclude approved support activity and authorised tickets. | Preserve process/service/network evidence; active remote control is a critical override. |
| *DEV-02* | +4 | First 90 days | Developer tunnels and legitimate support may be expected. | Inspect signer, command line, parent process and destination. |
| *DEV-03* | +5 | First 90 days | Software EDR may not see remote hardware. | Correlate NAC, switch, DHCP, USB and physical evidence. |
| *DEV-04* | +3 | First 90 days | VPN, travel, VDI and mobile use can be legitimate; MFA success is not identity proof. | Review reset/recovery context and establish the normal access path. |

| | | | | |
|---|---|---|---|---|
| *DEV-05* | +3 | First 90 days | Personal sign-in or synchronisation alone does not score. | Exclude benign personal use, testing and support before escalating. |

*Table 33. Signal guardrails: device and access continuity*

## MISSION AND DATA BEHAVIOUR — FIRST 90 DAYS

| SIGNAL | PTS | PRIMARY STAGE | KEY GUARDRAIL | NEXT ACTION |
|---|---|---|---|---|
| MIS-01 | +4 | First 90 days | One accidental decoy interaction is not exfiltration. | Review depth, sequence, destination and repetition. |
| MIS-02 | +5 | First 90 days | Build, backup and migration activity can be legitimate. | Validate with the manager; active exfiltration is a critical override. |
| MIS-03 | +3 | First 90 days | Overbroad entitlement or legitimate tasking can explain access. | Validate manager expectations and reduce unnecessary access regardless of attribution. |
| MIS-04 | +3 | First 90 days | Shift work, shared infrastructure and personal browsing can be benign. | Compare against approved work/session baselines before escalation. |

*Table 34. Signal guardrails: mission and data behaviour*

## ADMINISTRATION AND FINANCE — ONBOARDING AND FIRST 90 DAYS

| *SIGNAL* | PTS | PRIMARY STAGE | KEY GUARDRAIL | NEXT ACTION |
|---|---|---|---|---|
| *ADM-01* | +2 | FIRST 90 DAYS | ADMINISTRATIVE CHANGES ARE COMMON AND LEGITIMATE. | VERIFY THROUGH A KNOWN CHANNEL AND EXAMINE RELATED IDENTITY/DEVICE EVIDENCE. |
| *ADM-02* | +2 | ONBOARDING / FIRST 90 DAYS | BENEFITS UNFAMILIARITY DOES NOT SCORE; USE OBJECTIVE RECORD CONFLICT ONLY. | APPLY THE CORRECTION ROUTE AND LEAVE UNRESOLVED EVIDENCE OPEN WITH AN OWNER. |
| *ADM-03* | +4 | ONBOARDING | A PROVIDER MAY PROPOSE A LEGITIMATE SUBSTITUTE ONLY THROUGH THE APPROVED ROUTE. | PAUSE ACCESS FOR UNAPPROVED SUBSTITUTION AND REVIEW THE WIDER SUPPLIER POPULATION. |

*Table 35. Signal guardrails: administration and finance*

## CASE HANDLING AND CLOSURE

| Rule | Operational instruction |
| --- | --- |
| Evidence, review and closure | Record observable facts and the candidate/employee explanation; reference rather than copy sensitive source material; keep scoring human-led; and before closing record the decision, next action, owner, due date, retention/deletion owner and final access state. Do not infer nationality or label the person a DPRK operative. |

At closure, restrict access to the case team. Do not share the score or investigative mechanics with the candidate or employee.

☐ Evidence references, root-cause grouping and explanation are complete.

☐ Tier, decision, owner, due date, retention/deletion and case access are complete.

# SOURCES AND FURTHER READING


1. HM Treasury, Office of Financial Sanctions Implementation, “North Korean IT Workers Advisory: Signs to Watch For” (12 September 2024). https://www.gov.uk/government/publications/north-korean-it-workers-advisory-signs-to-watch-for
2. Google Threat Intelligence Group, “DPRK IT Workers Expanding in Scope and Scale” (1 April 2025). https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale
3. Microsoft Threat Intelligence, “Jasper Sleet: North Korean Remote IT Workers’ Evolving Tactics to Infiltrate Organisations” (30 June 2025). https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/
4. Federal Bureau of Investigation, “North Korean IT Workers Conducting Data Extortion” (2025). https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-workers-conducting-data-extortion
5. US Department of Justice, “Two US Nationals Sentenced for Facilitating Fraudulent Remote Information Technology Worker Schemes” (6 May 2026). https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology-worker-0
6. Okta Threat Intelligence, “How AI Services Power the DPRK’s IT Contracting Scams” (24 April 2025). https://sec.okta.com/articles/2025/04/GenAIDPRK/
7. Palo Alto Networks Unit 42, “False Face: Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation” (21 April 2025). https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/
8. Information Commissioner’s Office, “Pre-employment Vetting of Candidates”. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/recruitment-and-selection/pre-employment-vetting-of-candidates/
9. Information Commissioner’s Office, “Data Protection and Monitoring Workers”. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/
10. UK Government, “Code of Practice for Employers: Avoiding Unlawful Discrimination While Preventing Illegal Working”. https://www.gov.uk/government/consultations/amendments-to-the-home-office-code-of-practice-for-employers/code-of-practice-for-employers-avoiding-unlawful-discrimination-while-preventing-illegal-working
11. Information Commissioner’s Office, “What Are Storage and Access Technologies?”. https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/what-are-storage-and-access-technologies/
12. SANS Institute, Blueprint podcast, “Infiltration Alert! How to Catch Fake IT Employees in Your Network with Zak Stufflebeam” (5 January 2026). https://www.sans.org/podcasts/blueprint
13. Participating governments and agencies, “Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers” (31 July 2026).
14. Recorded Future, conference presentation on identifying and investigating DPRK IT worker activity, YouTube (accessed 4 August 2026). https://www.youtube.com/watch?v=7kucQe6tZF8
15. ANY.RUN, “Smile, You’re on Camera! Part 2: Hiring Lazarus APT’s IT Workers in a Fake DeFi Startup” (10 August 2026). https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation-part-two/
16. Genians Security Center, “Kimsuky Integrates AI into Attack Operations, From AI-Generated Decoy Documents to a Local LLM” (10 August 2026). https://www.genians.co.kr/en/blog/threat_intelligence/kimsuky_ai_llm
17. SentinelLABS, “DPRK IT Workers | A Network of Active Front Companies and Their Links to China” (21 November 2024). https://www.sentinelone.com/labs/dprk-it-workers-a-network-of-active-front-companies-and-their-links-to-china/
18. DTEX Systems, i3 Threat Advisory, “Identifying North Korean IT Workers: Key Threat Indicators” (updated 14 May 2025). https://www.dtex.ai/resources/i3-threat-advisory-inside-the-dprk/
19. GetReal Security, “Enterprise Account Recovery: Defending Against Credential Reset Attacks” (3 April 2026). https://www.getrealsecurity.com/resources/enterprise-account-recovery-defending-against-credential-reset-attacks

BCON COLLECTIVE
By Bridewell

+44 (0)3303 110 940
hello@bridewell.com
bridewell.com