CYBEHAVE ACADEMY · SPECIALIST

Behavioural Science for Security Architects

Course workbook

Designing controls around how people actually work.

Build Behaviour. Build Culture. Build Resilience.

This workbook belongs to

Organisation and role

One control I own, and one I am about to design

cybehave.com/training · © 2026 CyBehave. All rights reserved. For use alongside the Behavioural Science for Security Architects video course.

BEFORE YOU START

How to use this workbook

This is the specialist course for the people who decide what a control asks a person to do. The workbook follows the ten videos in order, holds every template the videos refer to, and ends with the eight quizzes and their answers. By the end you will have written the ask for a control you own, counted a role's security asks per day, started a workaround catalogue, planned a five-user test, run the substitution test on a design under pressure, and written a behavioural design record for a control you are about to ship.

Five ways to get the most from it

1. **Bring two controls.** One you own and one you are about to design. Every section has a "Your next control" box.
2. **Write the ask first.** Who, does what, when, instead of what. Most of the course follows from that sentence.
3. **Count by shadowing, not by listing.** The asks-per-day count in module 2 is the single most useful number you will produce.
4. **Take the quizzes.** Scenarios, not definitions. Check the key and read the explanation for anything you missed.
5. **Do one thing per module.** Write the ask. Count the asks. Start the catalogue. Audit the friction. Audit the prompts. Book the test. Run the substitution test. Write the record.

The course at a glance

Module	Title	Tools in this workbook
0	Welcome	Why every control is an ask; meet Mei.
1	Every Control Is a Behaviour	The control-as-ask card; the COM-B dependency sheet; the assumption sentence.
2	The Compliance Budget	The asks-per-day count; the compliance-budget ledger.
3	Workarounds as Data	The three-responses sorter; the workaround catalogue; the keeps / protects / drops sheet.
4	Defaults, Paths and Friction	The two-paths step count; the defaults-and-friction audit.
5	Warnings, Prompts and Fatigue	The prompt audit; the anatomy scorecard.
6	Testing a Control with Real Users	The five-user test plan and log; the measure sheet.
7	Designing for the Moment of Attack	The brace patterns; the moment-of-attack review; the substitution test for designs.
8	The Behavioural Design Record	The seven-line record template; the six-question review checklist; the HEROES map; the annual review sheet.
9	Close	Eight ideas; Monday list; glossary; further reading; quiz answers.

Three lines you will hear again

Every control is an ask. Write down who you are asking. · The workaround is the design proposal. · Secure enough, then as easy as possible.

WORKED EXAMPLE

Meet Mei

Mei Chen is principal security architect at Arden Water, a regional water utility of 2,600 people: a control room of 180 running water and wastewater around the clock, 640 field engineers with tablets and vans, 400 contractors, and an IT estate and an operational technology estate that are supposed to be separate and are not quite. She came from a bank where controls were designed in a room and rolled out by email. The course follows her first year of designing controls with the people who have to live with them.

The five threads the course returns to
The shared control-room login (modules 1, 3, 4): fourteen screens, one generic account, a password on a sticky note, because the screen lock fired every five minutes and an operator locked out mid-alarm is a safety risk. Badge-tap, per-person sessions, a shift-matched timeout: shared logins from 100% to zero in eleven weeks.
The MFA push at 05:40 (modules 2, 5, 7): a field engineer approved a push he had not started, because he received eleven a day and had learned to press yes. Number matching, longer sessions on managed tablets, deny as a report: pushes from 11 a day to 2.
The USB in the control room (modules 2, 4, 6): firmware and logs moved by stick because the portal needed three approvals and a day. One step for signed vendor files, the slow path before the block: portal use from 12 to 310 a month; ports locked in month seven, unnoticed.
The payee-change hold nobody used (modules 7, 8): a separate system, a second approver who was never there, no way to verify from the screen. Built into the payment screen with the master-record number and any of four approvers: used on 3% of changes to 100%.
The remote-access redesign, tested first (modules 6, 8): five field engineers at a depot found four of six blockers in ninety minutes; task time from 9 minutes to 48 seconds; the design record for it became the template.

Use Mei as a mirror

Each time an Arden Water card appears, ask: what is my equivalent? What does my control assume about the person? What is my shared login, my eleven prompts, my USB stick?

MODULE 1

Every Control Is a Behaviour

Key ideas from the video

- A control is a behaviour change request. Write it as an ask: who, does what, when, instead of what. Written like that, most controls predict their own failure.
- COM-B for control design: every control depends on capability, opportunity or motivation. Name the one it leans on hardest. Most failures live in opportunity; a control that depends on motivation works only when nobody is busy.
- The behavioural assumption: the person the control assumes, by device, time, location, attention, authority and frequency. Read the sentence to somebody with the role. If they laugh, you have found the defect.
- Controls fail in the assumption nobody checked, not in the person. The incident report says "user shared credentials"; the design review should have said "control assumed a desk worker".
- The substitution test for designs: would three other people in that role, on that shift, with that device, have done the same? If yes, the control failed and will again.

Template: the control-as-ask card

Line	Control one (the one I own)	Control two (the one I am designing)
The ask: who, does what, when, instead of what		
The dependency: capability / opportunity / motivation, and which carries the weight		
The assumption: device, time, location, attention, authority, frequency		
The prediction: where, when and by whom this will be worked around		
Read to (name, role) and what they corrected		

Mei writes the ask for the screen lock

"A control-room operator, every five minutes of inactivity, on each of up to fourteen screens, re-enters a twelve-character password, instead of watching the alarm." Dependency: opportunity. Assumption: a desk worker with one screen and time to spare. Prediction: a shared account within a week, which is what had happened four years earlier. Substitution test: the shift lead laughed.

Redesign with two shift leads: badge-tap to unlock, per-person sessions that follow the operator between screens, a lock timeout matched to the shift pattern. Shared-account logins 100% to zero in eleven weeks, without a policy email.

Your next control

Write the ask for your control and read it to one person who has the role. Note what they correct.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Take one control you own. Write its ask in one sentence: who, does what, when, instead of what. Could the person it asks recognise themselves in it?

2. Which COM-B component does that control depend on most: capability, opportunity or motivation? What happens to the control if that component is missing at 05:40?

3. List the assumptions the control makes about the person: their device, their time, their location, their attention, their authority. Which one has never been checked?

4. Who was in the room when that control was designed, and who lives with it? If those are different people, what did the second group never get to say?

5. Which of your controls fails most often, and is the failure in the person or in the assumption?

Module 1 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. The course says to write every control as an "ask". What are the four parts of the ask?

A Threat, control, residual risk, owner

B Confidentiality, integrity, availability, accountability

C Policy, standard, procedure, guideline

D Who, does what, when, instead of what

2. A control-room screen lock fires every five minutes across fourteen screens. Which COM-B component does the control depend on, and why does it fail?

A Capability: operators cannot remember passwords

B None; the lock is a technical control with no behavioural dependency

C Opportunity: the environment (an alarm in progress, fourteen screens, no time) does not allow the behaviour, whatever the operator wants

D Motivation: operators do not care about security

3. What is the "behavioural assumption" the course asks you to write down?

A The assumption that the control meets the standard

B The person the control assumes: their role, device, location, time, attention, authority and how often they face the ask

C The assumption that users will follow policy if trained

D The attacker's assumed capability

4. An incident report says "user shared credentials". What does the course say the design review should have said?

A "Control assumed a desk worker": a sentence about a decision, not about a person

B "User requires retraining"

C "Policy was not communicated clearly enough"

D "User should be disciplined"

5. What is the substitution test, applied to a design?

A Could a different technology substitute for the control?

B Would the control work if a different team owned it?

C Could the user be replaced by automation?

D Would three other people in that role, on that shift, with that device, have done the same? If yes, the control failed and will fail again

6. What does the course call "the first design question"?

- **A** Which standard does this control satisfy?
- **B** What does this control cost to implement?
- **C** What does this ask a person to do, when, under what pressure?
- **D** Which threat does this control mitigate?

MODULE 2

The Compliance Budget

Key ideas from the video

- Beautement, Sasse and Wonham (2008): people comply with security up to a threshold of cumulative cost, then stop. The budget is per person, not per control, so every control competes with every other. The organisation can move the threshold.
- Herley (2009): rejecting security advice is often rational, because the cost of following it, summed across everyone every day, exceeds the rare direct loss it prevents. If you cannot show the protection is worth the budget, the control is the problem.
- Count the asks by shadowing one person for one shift: logins and re-logins, prompts, warnings, approvals, portals, rules remembered. The control list says six; the day says fourteen.
- The ledger: for every ask, cost per occurrence, occurrences per day, what it protects, how often that threat reaches the role, and the alternative. Refund what buys nothing; spend it where it matters.
- Raises the threshold: visible benefit, fast feedback, fit, respect. Drains it: asks that protect nothing visible, asks that fail, blame when the budget runs out.

Template: the asks-per-day count (shadow one shift)

Time	The ask (what security asked them to do)	Self-initiated? (Y/N)	Seconds	What they did

Template: the compliance-budget ledger

Ask	Cost per occurrence (s)	Per day	Protects against	How often that reaches this role	Automate / remove / redesign / keep

Fourteen asks before lunch

A Tuesday in a van, 06:00 to 13:00: four logins (two from timeouts), five MFA pushes (one self-started), two app warnings, a VPN reconnection at every site, an abandoned transfer-portal request, and a rule remembered (no photos on the phone), so she used the phone. The pushes and timeout logins consumed most of the budget and protected against a threat that had reached a field engineer once in three years. The transfer control, protecting the plant network, was the one abandoned.

Refunded: session length on managed tablets from one hour to the shift; VPN always-on; the two app warnings removed. Asks per day 14 to 5 by year end. Spent on: the one-step portal and number matching. Mei's rule: no new control without the asks-per-day count for the role.

Your next control

Shadow one person in the role your control lands on, and count. Then place your control on the ledger.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Count the security asks one role in your organisation faces in a normal day: prompts, logins, approvals, warnings, forms. Do it by shadowing, not by listing the controls.

2. For each ask, what does it protect, and how often does that protection matter? Which asks are spending budget on nothing?

3. Where in your estate has compliance visibly run out: the shared password, the always-approved prompt, the policy everyone knows and nobody follows?

4. Which one ask could you remove this quarter without lowering protection, and what would you spend the refund on?

5. If a user told you that ignoring one of your controls was the rational choice, could you prove them wrong with numbers?

Module 2 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What did Beautement, Sasse and Wonham find about compliance with security policy?

A Compliance is determined by personality and cannot be changed

B People never comply with security policy

C People comply up to a threshold of cumulative cost, then compliance wanes; the organisation can move the threshold

D People comply fully if the policy is clear

2. Herley argued that users rejecting security advice is often rational. Why?

A Users cannot understand the advice

B The cost of following the advice, summed across everyone every day, exceeds the direct losses it prevents, which are rare and small

C Users are too lazy to follow advice

D Security advice is always wrong

3. The course says to count security asks by shadowing a person, not by listing controls. Why?

A Because the control list says six and the day says fourteen: timeouts, re-logins, repeated prompts and abandoned portals never appear on the list

B Because the control list is confidential

C Because shadowing is faster

D Because users cannot be trusted to report controls

4. Which column does the compliance-budget ledger NOT include?

A Cost per occurrence and occurrences per day

B What the ask protects against and how often that threat reaches the role

C The alternative: automate, remove, redesign, or keep and pay

D The user's performance rating

5. Mei shadowed a field engineer and counted fourteen asks before lunch. Which ask was being abandoned, and what did that tell her?

A The lock screen, because engineers are careless

B None were abandoned; the engineer complied with all fourteen

C The transfer portal, which protected the plant network: the budget had been spent on prompts and timeouts that protected little, so the one that mattered was skipped

D The VPN, because engineers do not understand networking

6. Which of these RAISES the compliance threshold, according to the module?

A Adding a warning to every ask

B Visible benefit, fast feedback, fit with the device and moment, and being asked before the control was imposed

C More frequent reminders about the policy

D Disciplinary consequences for non-compliance

MODULE 3

Workarounds as Data

Key ideas from the video

- Three responses to a control that does not fit: comply at a cost (tolerable, for now), bypass (the protection was not visible), or work around (the person wanted security and you did not give them a usable way). Kirlappos, Parkin and Sasse (2014) called the third "shadow security".
- Read every workaround as a design proposal: what it keeps (the job), what it protects (the person's threat model), what it drops (your requirement). The redesign keeps, protects and adds back, at lower cost than the workaround.
- Find them: ask in person with no notebook; read helpdesk tickets for "can't" and "how do I get round"; read logs for the shape of one; ask the Champions; walk round. Make reporting one safe, from the top.
- The rule: fix the control first, never the person. Close a workaround only after a usable alternative exists and has been tested. Closing it first produces the next, less visible workaround.
- Some workarounds beat the control. Adopt them and name their authors: the first adoption brings every other workaround out of the shadows.

Template: the three-responses sorter

Control	What people do instead	Comply at a cost / bypass / workaround	What that tells me

Template: the workaround catalogue

#	Workaround (as described)	Control it substitutes for	Keeps	Protects	Drops	Who / how many / how often	Source	Decision

#	Workaround (as described)	Control it substitutes for	Keeps	Protects	Drops	Who / how many / how often	Source	Decision

Source: interview, ticket, log, Champion, walk round. Decision: redesign, adopt, tolerate, close (after a tested alternative).

Thirty-seven entries, and the USB stick

29 from interviews and Champions, 8 from logs. Identity and access 14, file transfer 9, remote access 6, physical 5, payments 3. Workaround 22, bypass 11, comply-at-a-cost 4. Entry 7: engineers moved firmware by stick because the portal needed three approvals and a day. Keeps: the job done on site. Protects: sticks only from the vendor's sealed pack. Drops: scanning, logging, revocation.

Four entries adopted as the control, including the shift handover book and the engineers' vendor list; their authors named at the engineering forum. The catalogue grew by eleven volunteered entries the following month. Every control in the standard is checked against the catalogue once a year; four retired.

Your next control

Enter the three workarounds you already know about, with keeps / protects / drops, and write the control each one implies.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Name three workarounds you already know about in your estate. For each: what control does it bypass, what does it tell you the person actually needed, and what has been done about it so far?

2. How would somebody in your organisation report a workaround today without getting into trouble? If there is no such route, what would one look like?

3. Take one workaround and write the control it implies: the one the user would have designed if asked.

4. Which of your controls has a workaround that is, in practice, more secure than the control itself?

5. Who in your organisation sees workarounds first: the helpdesk, the Champions, the auditors, the attackers? How do they reach you?

Module 3 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. Kirlappos, Parkin and Sasse described "shadow security". What is it?

A The attacker's view of the organisation

B The third response to a control that does not fit: people build their own substitute with some protection they chose, invisible to official security

C A covert security team

D Security controls hidden from users

2. Which three things does the course say to read in any workaround?

A What it keeps (the job), what it protects (the person's threat model), and what it drops (your requirement)

B Who did it, when, and how to stop them

C The policy breached, the sanction, and the retraining needed

D The cost, the risk, and the audit finding

3. What is the rule when you find a workaround?

A Close the workaround immediately and retrain the user

B Report the user to their manager

C Add the workaround to the risk register and move on

D Fix the control first, never the person; close the workaround only after a usable alternative exists and has been tested

4. Which of these is a way the course suggests finding workarounds?

A Run a disciplinary audit

B Wait for the next incident

C Read helpdesk tickets for "can't", "won't let me" and "how do I get round"

D Monitor employees' personal social media

5. The finance team phoned a colleague before any payee change because the official second approver was never there. What did Mei do?

A Ignored it as a minor deviation

B Adopted the phone call as the control, removed the broken approver role, and named the people who designed it

C Disciplined the team for not using the official process

D Made the official approver mandatory and blocked payments without them

6. What happened to Mei's catalogue after the first workaround was adopted and its author named?

- **A** It grew by eleven entries in a month, most of them volunteered
- **B** It was closed for legal reasons
- **C** Nothing changed
- **D** Staff stopped reporting for fear of being named

MODULE 4

Defaults, Paths and Friction

Key ideas from the video

- Draw the two paths, the secure way and the way people go, and count the steps. Nobody chooses nine steps over two for a routine task; change the step count, not the person.
- Secure by default: the NCSC principle that security should never compromise usability. Secure enough, then maximise usability. The default is the strongest control you own, because most people never change one.
- Friction belongs on the rare action with a large, hard-to-reverse consequence, on the action an attacker needs and a user seldom does, and at the moment of attack. It does not belong on the hundred-times-a-day action.
- Slower and visible before impossible: a block moves the workaround out of sight; a slow path tells you who still needs the old way. Build the easy secure path, watch it win, then slow the old path, then close it.
- Remove steps from the secure path: pre-fill, put the action where the work is, replace clear approvals with rules, collapse factors into one gesture, extend trust already established. Count again afterwards.

Template: the two-paths step count

Task (as the person would say it)	The secure path: steps, waits, systems	Step count	The path people take	Step count	What to remove from the secure path

Template: the defaults-and-friction audit

Action	How often per person per day	Consequence if wrong (size, reversibility)	Friction today (steps, waits, prompts)	Friction should be: none / low / high	Default today: secure / vendor / none

Action	How often per person per day	Consequence if wrong (size, reversibility)	Friction today (steps, waits, prompts)	Friction should be: none / low / high	Default today: secure / vendor / none

The portal that won

Before: nine steps, two approvers, a day's wait, corporate network only; 12 portal transfers a month; sticks everywhere. The redesign, with three engineers on the group: one step for a signed file from a vendor on the master record, under 2 GB, scanned inline, reachable from the plant network, the button in the work-order app pre-filled with the vendor from the job. Unknown sources kept the approvals.

Month four: the slow path (USB asks for a reason, logs it, shows the portal button; reasons read weekly, two real gaps fixed). Month seven: 310 portal transfers a month, three USB reasons, all moved into the portal; ports locked; nobody noticed. "The control that won was not more secure than the old one. It was shorter."

Your next control

Count the steps on both paths for your control, and name one step you will remove this month.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. For one task your people do daily, draw the two paths: the secure way and the way they actually go. Count the steps on each. Which is shorter?

2. Where in your estate is friction sitting on a hundred-times-a-day action, and where is a rare, risky action completely frictionless?

3. Which of your controls makes the unwanted action impossible when it could make it slower and visible instead? What would you learn from the slower version?

4. What is the default in your three most-used systems: the secure option, or the one the vendor shipped?

5. Name one step you could remove from the secure path this month without lowering protection.

Module 4 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. The secure transfer path had nine steps and a day's wait; the USB stick had two steps. What does the course say to change?

A The step count: make the secure path the shortest one, because nobody chooses nine steps over two for a routine task and no training changes that

B The training, so people understand why nine steps are necessary

C The policy, to prohibit USB sticks more firmly

D The people, by hiring more compliant engineers

2. What does the NCSC Secure by Default principle quoted in the module say about usability?

A Usability must always be sacrificed for security

B Usability is the user's responsibility

C Security and usability are unrelated

D Security should never compromise usability: make it secure enough, then maximise usability

3. Where does the course say friction belongs?

A On the hundred-times-a-day action, because that is where most risk is

B Nowhere; friction is always bad

C On the rare action with a large, hard-to-reverse consequence, and on the action an attacker needs but a user seldom does

D On every action, to keep people alert

4. Why does the course prefer making an unwanted action "slower and visible" to making it impossible?

A Because slower actions are always more secure

B Because a block moves the workaround somewhere you cannot see it, while a slow path tells you who still needs the old way and why

C Because blocking is technically difficult

D Because users have a right to bypass controls

5. Which of these is a way of removing steps from the secure path?

A Pre-fill what the system already knows, put the action where the work is, replace clear-cut approvals with rules, and extend trust already established

B Add a confirmation dialog to each step so users slow down

C Require a second factor at every step

D Move the secure action to a dedicated portal

6. When did Mei lock the USB ports, and why then?

A On day one, to force adoption of the portal

B Never; USB remained the main route

C Before the portal was redesigned, as a quick win

D In month seven, after the portal had reached 310 transfers a month and USB reasons were down to three legitimate cases, all moved into the portal

MODULE 5

Warnings, Prompts and Fatigue

Key ideas from the video

- Akhawe and Felt (2013), over 25 million real browser warnings: 70% of Chrome's SSL warnings clicked through against 33% of Firefox's, and a tenth to a quarter of malware warnings. Same users, same threats; the design changed behaviour by a factor of two.
- Habituation: a prompt seen eleven times a day for the same safe outcome is not read on the twelfth. You built it. A prompt answered in under a second is a reflex, and a reflex is a lever.
- The anatomy of a prompt that works: rare, specific, consequential, actionable, safe action first. A warning the person cannot act on is noise: log it, block it, or fix it.
- The second factor is a prompt. "Approve?" trains approval; number matching requires the real request. Fewer prompts, context on the prompt, and "no" as a one-tap report with a thank-you.
- The prompt audit: how often one person sees it, how fast they answer, what happens on "no", whether the system could decide instead, and the anatomy score.

Template: the prompt audit

Prompt	Seen per person per day	Median response time	What "no" does	Could the system decide?	Anatomy score (0 to 5)	Rewrite / remove / keep

Template: the anatomy scorecard (one prompt)

Criterion	Yes / no	The rewrite
Rare: fires only when something is actually unusual		
Specific: says what is wrong in the words the role uses		
Consequential: says what happens next, either way		

Criterion	Yes / no	The rewrite
Actionable: offers a thing the person can do that solves it		
Safe action first: default, prominent, the button Enter presses		

The push at 05:40

A field engineer approved a push he had not started; the attacker had a reused password; forty minutes of mailbox access before he reported it himself. The audit: a median of 11 pushes a day, 2 self-initiated; median time from push to approval 0.8 seconds. The incident report draft said "user approved unrecognised prompt". Mei rewrote it: "design trained approval".

Redesign: number matching on every push; sessions on managed tablets extended to the shift; location and application on the prompt; deny as a one-tap report with a thank-you. Pushes 11 to 2 a day; response time 0.8 to 6 seconds; 14 denied prompts reported in the first quarter, 3 real. The card: "A prompt you did not start is a report. Tap no. We will say thank you."

Your next control

Audit the one prompt your control shows most often. Score it, and rewrite or remove it.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. How many security prompts does one of your users see in a day, and how many of those did they start themselves? Which figure have you measured rather than guessed?

2. Take your most common warning. Does it say what is wrong, what will happen, and what to do, in that order, in words the role uses? Is the safe action the first button?

3. Which prompts in your estate are shown so often that nobody reads them? What do they protect, and could that protection be delivered without a prompt?

4. Does your second factor require the person to do something only the real request could produce (a number match, a code typed in), or just to press yes?

5. What happens when somebody says no to one of your prompts? Is it a report, or just a closed dialog?

Module 5 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. In Akhawe and Felt's study of over 25 million real browser warnings, what share of Chrome's SSL warnings did users click through, compared with Firefox's?

A About 5% in both

B About 99% in both

C About 33% in Chrome and 70% in Firefox

D About 70% in Chrome and about 33% in Firefox: the same users and threats, a different warning design

2. What is habituation, and who builds it?

A A browser setting users enable

B An attacker technique unrelated to design

C The brain stops processing a prompt seen often with the same safe outcome; the design built it by firing the prompt on every login, file and timeout

D A user's personal laziness, which training can fix

3. Which is NOT part of the anatomy of a prompt that gets a decision?

A Safe action first, as the default and prominent button

B Frequent, so users remember it

C Specific, in the words the role uses

D Consequential, saying what happens next either way

4. Why does number matching defeat the MFA fatigue attack where a simple "approve?" push does not?

A Because the phone asks for a number shown only on the real login screen: no number, no approval, and no reflex to exploit

B Because it sends more notifications

C Because it requires a longer password

D Because it blocks all logins from new devices

5. What does the course say should happen when a user says "no" to a prompt?

A Nothing; the dialog closes

B The user is locked out

C The prompt is shown again

D It becomes a one-tap report to security, and the person is thanked

6. At Arden Water, the median time from MFA push to approval was 0.8 seconds. After the redesign it was 6 seconds. Why did Mei count the increase as success?

A Because it reduced the number of logins

B Because it showed users were confused

C Because six seconds meant people were reading the prompt and matching the number, where under a second had been a reflex

D Because slower logins are always more secure

MODULE 6

Testing a Control with Real Users

Key ideas from the video

- Controls are tested against threats, standards and auditors, and almost never against a real person doing the real task. The five-user test costs ninety minutes and finds most of what will go wrong.
- Five people who actually have the role, the real task as they would describe it, their device, their place, one at a time, thinking aloud. You do not help until they are stuck for two minutes, and then you note it.
- Count: completion unaided, time against baseline, errors, help needed and at which step, the workaround they try, and the words they use. Write the stop line first and agree it with whoever can delay the rollout.
- Fix the top three problems, retest with five new people, then pilot with a comparison (Running Behavioural Experiments has the method). Roll out last, with the numbers in the record.
- A control without a behaviour measure is a hope. Every control ships with one measure, a baseline, a workaround signal, an owner, and a stop number.

Template: the five-user test plan

Line	Entry
The control	
The task, as the user would say it	
The five people (role, tenure, site), and who is excluded	
Device, place, time	
Baseline time for the task without the control	
The stop line (completion, time), and who agreed it	
Date, facilitator, note-taker	

Template: the five-user test log

User	Completed unaided? (Y/N)	Time	Errors (step)	Help needed (step)	Workaround tried or described	Words they used
1						
2						
3						
4						

User	Completed unaided? (Y/N)	Time	Errors (step)	Help needed (step)	Workaround tried or described	Words they used
5						

Template: the measure that ships with the control

Line	Entry
The behaviour counted	
Baseline before rollout	
The workaround signal (what rises if the control does not fit)	
Where it is read, by whom, how often	
The stop number: the value that means the control has failed	

Ninety minutes at the depot

The remote-access redesign: five engineers at the Northgate depot, their own tablets, "check the pump telemetry at site 14", one at a time, thinking aloud; stop line agreed with the head of operations. Found: 4 of the 6 blockers that would have reached production: a certificate prompt nobody understood, a site list in asset-register order, a session that dropped when the tablet slept, an "approve on phone" step that assumed the phone was not in the van.

After two loops: five of five unaided; 9 minutes to 48 seconds; the phone step removed on managed tablets. Piloted at two depots against two for six weeks. Shipped with one measure (remote sessions per engineer per week against control-room telemetry calls), one stop number, and one line from the engineers: "Tested by five of us at Northgate. It works in the van."

Your next control

Book the five-user test for your next control, write the stop line, and name who agreed it.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Which control did you last roll out without watching a single real user do the real task with it first? What did you learn in the first month that ninety minutes would have shown you?

2. Pick a control you are about to ship. Write the task as the user would describe it, not as the control describes it. Who are the five people you will watch?

3. What will you count: completion, time, errors, the workaround invented on the spot? What number would make you stop the rollout?

4. What behaviour measure will go live on the same day as the control, and where will it be read?

5. If the five-user test finds the control unusable, who has the authority to delay the rollout, and have they agreed to in advance?

Module 6 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What does the five-user test involve?

A A survey sent to five hundred users

B Five managers approving the control

C Five people who actually have the role, doing the real task on their own device in their own place, one at a time, thinking aloud, in about ninety minutes

D Five security team members reviewing the design

2. Why five users, according to the course?

A Because more would be too expensive

B The usability research tradition since Nielsen: the first five find most of the serious problems and the sixth mostly repeats them; fix, then test five more

C Because five is the legal minimum

D Because statistical significance requires exactly five

3. What is the "stop line", and when is it agreed?

A A result (for example fewer than four of five completing unaided) that means the control does not ship; agreed with whoever can delay the rollout, before the test

B The point at which the test session ends

C The deadline for rollout

D The maximum budget for the control

4. Which of these is something the course says to count in the test?

A The user's security training score

B The number of times the user praises the design

C The user's job grade

D The workaround the person tries, or says they would try, when the control does not work, written down verbatim

5. What does the course say about a control without a behaviour measure?

A It can be measured by audit findings instead

B It needs a survey after a year

C It is a hope: every control ships with one measure of the behaviour it depends on, a baseline, a workaround signal and an owner who reads it

D It is acceptable if the control is technical

6. What did ninety minutes with five engineers at the Northgate depot find?

A That the test was a waste of time

B Four of the six blockers that would have reached production, including a certificate prompt nobody understood and a session that dropped when the tablet slept

C That the control was perfect and needed no changes

D That engineers could not be trusted with remote access

MODULE 7

Designing for the Moment of Attack

Key ideas from the video

- The attacker is a choice architect: they design the moment, the pressure, the path and the person's state. Anything that depends on the person pausing, checking or refusing is theirs to remove, so those have to be in the system.
- Five braces built into the system: the hold; the out-of-band confirmation from a channel you control; the thing only the real request has; the four-eyes rule that actually works (any of four, reachable from a phone); the cooling-off on new destinations and devices.
- Verification as architecture, not advice: the master-record number and a Call button on the screen, the approval in the approver's app with the full detail. One tap, from inside the process, using nothing the request supplied.
- The substitution test for designs: three ordinary people in the role, the worst realistic moment, the attacker's request. If stopping it depends on one of them saying no, the control does not hold.
- Design the rushed path on purpose: the hold still applies and can be escalated inside the system; the refusal is a button; everything done under pressure is logged as context, not blame.

Template: the brace patterns, applied

Process (money, access or data)	The hold	Out-of-band channel we control	The thing only the real request has	Four-eyes that works	Cooling-off

Template: the substitution test for a design

Line	Entry
The process, the role, the worst realistic moment	
The attacker's request: pretext, pressure, channel	
Person 1 walked through: what happened	

Line	Entry
Person 2	
Person 3	
Does the system hold whatever they do? (yes / no)	
If no: which decision moves into the system, and how	

Template: the rushed path, designed

Question	Today	Designed
Does the hold still apply when the person is rushed? Can they see why and escalate inside the system?		
Can they verify in one tap using nothing from the request?		
Is the refusal a button the system presses for them?		
Is what they did under pressure logged as context, not blame?		

The payee-change hold, 3% to 100%

Before: a hold in a separate system, one named approver often away, no way to verify from the screen; used on 3% of changes; finance had a buddy-check workaround. The substitution test on paper: three officers, month end, a director's email with new supplier details. All three paid. The hold depended on remembering it existed.

Redesign: the hold built into the payment screen and applied by default; the master-record number with a Call button; any of four approvers with a mobile route; first payment to a new payee capped for 48 hours; the buddy check adopted as the approver step. Applied to 100% of changes; verification calls from the screen on 94%; four minutes added to a legitimate change; two fraudulent changes stopped in the first quarter. "Three officers, Friday 16:40, a director on the phone. The system holds whatever they do."

Your next control

Run the substitution test on your control at its worst moment. Write which decision moves into the system.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. For each process in your estate that moves money, access or data: what does it do when the person is being rushed by somebody senior? Is the pause in the process, or in the person?

2. Which of your verification steps use a channel the attacker could supply (a number in the email, a link in the message)? Which use one you hold (the master record, the directory, the badge)?

3. Where could a cooling-off period or a hold be built into a system this quarter, and what would it cost the legitimate case?

4. Run the substitution test on a design: three people in the role, Friday at 16:40, a convincing request from a director. Does the system hold, or does it rely on one of them saying no?

5. What does your incident process assume about the person at the moment of attack: calm, alone, with time? Which assumption fails first?

Module 7 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What does it mean to say the attacker is a "choice architect"?

A The attacker builds fake websites

B The attacker designs the moment, the pressure, the path and the person's state so that the easiest decision is the one they want; anything that depends on the person pausing is theirs to remove

C The attacker works in an architecture team

D The attacker chooses which system to target

2. Which of these is a brace built into the system, as the module describes them?

A A hold applied by default to any payee change, with the callback number shown from the master record and a Call button on the payment screen

B A poster saying "always verify unusual requests"

C An annual reminder email about invoice fraud

D A policy requiring staff to be suspicious of senior requests

3. Why does the course say "verify before you act" is a poster rather than a control?

A Because verification is impossible

B Because posters are more effective than controls

C Because users never read policy

D Because at 16:40 the known channel is in a drawer and the attacker's number is on the screen; verification works when it is one tap from inside the process using nothing the request supplied

4. A second approver who is a single named person, often away from their desk, is described in the module as what?

A Sufficient if documented in policy

B A technical control

C Not a control but a reason to bypass one; the working version is any of four named people, reachable by a route that works from a phone

D Best practice for segregation of duties

5. What is the substitution test applied to a design under pressure?

A Test whether the system can be substituted by a manual process

B Walk three ordinary people in the role through the system with the attacker's request at the worst realistic moment; if stopping it depends on one of them saying no, the control does not hold

C Replace the control with a different vendor's product

D Ask three architects whether the design is secure

6. After the redesign, the payee-change hold was applied to 100% of changes. Why?

A Because it was built into the payment screen and applied by default, so it was not optional

B Because staff were threatened with discipline

C Because a new policy was published

D Because finance staff received more training

MODULE 8

The Behavioural Design Record

Key ideas from the video

- The decision record holds context, decision and consequences, and never says who the control asks, what it assumes, what it costs, what people will do when it does not fit, whether anyone watched a real user, or how we will know it works.
- The seven behavioural lines: the ask; the actor and the moment; the COM-B dependency; the compliance cost; the expected workaround; the test; the measure and the stop number.
- The six-question review checklist, next to the threat model on the board's template. Any "no" is a return, not a rejection. Within a quarter architects answer them before they are asked.
- The programme gives the architect the behaviour catalogue, Champions, Team Pulse and the reporting route; the architect gives the programme the record, the measure, the intervention record and the workaround catalogue.
- In HEROES: the behaviour and its measure, the intervention, the Team Pulse item, the board pack. Not in HEROES: the records, the catalogue, the logs. Review every control annually against its measure, its catalogue entries and the asks-per-day count; retire what fails.

The behavioural design record (template)

Line	Entry
Control, owner, date	
1 The ask: who, does what, when, instead of what	
2 The actor and the moment: role, device, place, time, frequency, what else is happening	
3 The COM-B dependency, and what happens when it is absent	
4 The compliance cost: seconds, per day, against the role's asks-per-day count; what was refunded	
5 The expected workaround: what, who, how soon, how we will see it	
6 The test: five-user result; pilot comparison; substitution test under pressure	
7 The measure and the stop number: behaviour counted, baseline, where read, the failure value	
Read and recognised by (name, role)	

The six-question review checklist

#	Question	Yes / return
1	Has somebody who has the role read the ask and recognised it?	
2	Is the asks-per-day count for the role in the record, and did this control refund more than it costs?	
3	Is the secure path the shortest path? Step count against the most likely alternative	
4	Did five real users complete the real task unaided, and is the result in the record?	
5	Does the system hold at the moment of attack, whatever the person does? Substitution test written up?	
6	Is there a behaviour measure, live from day one, with a stop number and an owner?	

Template: the HEROES map

This course	In HEROES	Ours
The behaviour each control depends on	Behaviour in the catalogue, with the control's measure as a direct measure	
Each control redesign	Intervention record with COM-B driver and APEASE pass	
"The secure way is the easy way"	Team Pulse item, by team, quarterly	
Champions surfacing workarounds and finding the five users	Champion tasks	
The measures over time	Board pack	
Design records, workaround catalogue, logs, test notes	Not in HEROES: kept by the architect	

Template: the annual review sheet

Control	Measure vs stop number	Catalogue entries pointing at it	Asks-per-day for its role	Keep / redesign / retire

Twenty-three records

23 behavioural design records in the year: 5 for the controls redesigned in this course, 11 for new controls, 7 written retrospectively for controls that had failed. The review board adopted the six questions in month six; returns fell from 9 of 14 to 2 of 12. The annual review retired four controls: a quarterly password change, a second approval on routine transfers, a banner nobody read, and a redundant VPN step.

In HEROES: five behaviours with the controls' measures as direct measures; five intervention records; "the secure way is the easy way" from 41% to 67% in the field-engineer teams. The line at the top of the template: "This control asks a person to do something. Before it ships, we will have written down who, watched five of them do it, counted what it costs them, and named the number that means it failed."

Your next control

Fill the seven lines for the control you are about to ship, and put the six questions on your review template.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Take your most recent architecture decision record. Does it say what the control asks a person to do? If not, add the seven behavioural lines now, from memory, and see which you cannot fill in.

2. Who reviews designs in your organisation, and does anyone on the review ask the behavioural questions? Who could, from next month?

3. Which three controls in your estate would fail the annual review against the workaround catalogue today?

4. Which behaviour measures from your controls could appear in HEROES beside the programme's other measures, and who would read them?

5. Who in the behaviour programme should see your design record before a control ships, and what would they add?

Module 8 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What does a typical architecture decision record never say, according to the course?

A Who the control asks, to do what, when; what it assumes about them; what it costs them; what they will do when it does not fit; whether anyone watched a real user; how we will know it works

B Which standard the control meets

C Which options were considered

D Who approved the decision

2. Which is one of the seven behavioural lines added to the record?

A The vendor's licence terms

B The network diagram

C The penetration test scope

D The expected workaround: what people will do when it does not fit, by whom, how soon, and how we will see it

3. On the six-question review checklist, what does a "no" mean?

A The architect is reassigned

B The control ships with a risk acceptance

C A return, not a rejection: the design goes back for the missing piece, such as a five-user test

D The control is cancelled

4. What does the behaviour programme give the architect, according to the module?

A The architecture decision records

B The behaviour catalogue, Champions who surface workarounds and find the five users, Team Pulse by team, and the reporting route

C Budget approval for all controls

D Penetration testing services

5. Which of these lives in HEROES, per the platform mapping?

A The behaviour the control depends on with the control's measure as a direct measure, the redesign as an intervention, the Team Pulse item and the board pack

B The architecture decision records and the workaround catalogue

C The identity and access logs

D The five-user test notes

6. What does the annual review check every control against, and what did it produce at Arden Water?

A The vendor roadmap; three controls upgraded

B The audit findings; no changes

C The budget; all controls renewed

D Its measure, its workaround catalogue entries and the asks-per-day count; four controls retired, including a quarterly password change and a banner nobody read

CLOSE

Close: What to Do on Monday

The course in eight lines

1. **Every control is a behaviour.** Who, does what, when, instead of what. Name the COM-B dependency. Write the assumption down.
2. **The compliance budget.** People comply up to a point. Count the asks per day by shadowing. Refund what buys nothing.
3. **Workarounds as data.** The workaround is the design proposal. Catalogue it. Fix the control first.
4. **Defaults, paths and friction.** Make the secure path the shortest. Friction only on the rare, risky action.
5. **Warnings, prompts and fatigue.** Rare, specific, consequential, actionable, safe action first. Number matching.
6. **Testing with real users.** Five people, the real task, ninety minutes, a stop line, a measure that ships with it.
7. **The moment of attack.** Put the pause, the channel and the refusal in the system.
8. **The behavioural design record.** Seven lines in every record; six questions at every review; one annual review.

Monday

Done	This week
☐	Write the ask for one control you own, and read it to someone who has the role
☐	Shadow one person for one shift and count the security asks
☐	Start the workaround catalogue with the three you already know about
☐	Book a five-user test for the next control you are about to ship, with a stop line
☐	Add the seven behavioural lines to one existing design record
☐	Put the six review questions on the design board's template, next to the threat model

Glossary

Term	Meaning in this course
The ask	A control written as a request: who, does what, when, instead of what.
COM-B dependency	The component (capability, opportunity, motivation) a control leans on hardest.
Behavioural assumption	The person a control assumes: device, time, location, attention, authority, frequency.
Compliance budget	The finite effort a person will spend on security; per person, not per control (Beautement, Sasse and Wonham).
Asks per day	The count of security asks one role faces in a shift, by shadowing.

Term	Meaning in this course
Shadow security	A substitute people build when a control does not fit, with protection they chose (Kirlappos, Parkin and Sasse).
Workaround catalogue	One row per workaround: keeps, protects, drops, who, source, decision.
Secure by default	Secure enough, then maximise usability; the default is the strongest control you own.
Friction	Steps, waits and prompts; a budget to spend on the rare, risky action only.
Habituation	The brain ceasing to process a prompt seen often with the same safe outcome.
Number matching	A second factor that requires something only the real request has.
Five-user test	Five people with the role, the real task, ninety minutes, before rollout.
Stop line / stop number	The test result that means no rollout; the measure value that means the control has failed.
Brace	A pause, channel or refusal built into the system so the attacker cannot remove it.
Behavioural design record	The seven lines added to the architecture decision record.

Further reading

- Adams, A. and Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12).
- Beautement, A., Sasse, M. A. and Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. NSPW 2008.
- Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. NSPW 2009.
- Kirlappos, I., Parkin, S. and Sasse, M. A. (2014). Learning from "Shadow Security": why understanding non-compliant behaviors provides the basis for effective security. USEC 2014.
- Akhawe, D. and Felt, A. P. (2013). Alice in Warningland: a large-scale field study of browser security warning effectiveness. USENIX Security 2013.
- Michie, S., van Stralen, M. M. and West, R. (2011). The behaviour change wheel. Implementation Science, 6(42).
- Nielsen, J. (2000). Why you only need to test with 5 users. Nielsen Norman Group.
- National Cyber Security Centre. Secure design principles; Secure by Default. ncsc.gov.uk.
- Wood, A. (2026). Brace.
- CyBehave Academy: Choice Architecture for Security; Running Behavioural Experiments; The Psychology of Social Engineering; Psychological Safety and Reporting Culture.

Notes

ANSWER KEY

Quiz answers

Four of six is a pass. Read the explanation for every question you missed, then go back to the template it points at.

Module 1: Every Control Is a Behaviour

#	Answer	Why
1	D Who, does what, when, instead of what	Written like that, a control predicts its own failure: "a control-room operator, every five minutes, re-enters a twelve-character password, instead of watching the alarm."
2	C Opportunity: the environment (an alarm in progress, fourteen screens, no time) does not allow the behaviour, whatever the operator wants	Most control failures live in opportunity. The operators' motivation was fine; the environment made the ask impossible during the moments that mattered.
3	B The person the control assumes: their role, device, location, time, attention, authority and how often they face the ask	Read the sentence to somebody who has the role. If they laugh, you have found the defect before the incident does.
4	A "Control assumed a desk worker": a sentence about a decision, not about a person	When the failure is written as a sentence about a person, the design is never the lesson and the next person fails the same way.
5	D Would three other people in that role, on that shift, with that device, have done the same? If yes, the control failed and will fail again	Applied to the shared login: the shift lead laughed. Almost every click, share or bypass passes the test, which is why almost every one is a design problem.
6	C What does this ask a person to do, when, under what pressure?	Before the threat model and the pattern. Answer it in writing and it becomes the first section of the behavioural design record.

Module 2: The Compliance Budget

#	Answer	Why
1	C People comply up to a threshold of cumulative cost, then compliance wanes; the organisation can move the threshold	The compliance budget is per person, not per control, so every control you add competes with every other for the same budget.
2	B The cost of following the advice, summed across everyone every day, exceeds the direct losses it prevents, which are rare and small	If you cannot show a control's protection is worth the budget it spends, the people ignoring it are not the problem.
3	A Because the control list says six and the day says fourteen: timeouts, re-logins, repeated prompts and abandoned portals never appear on the list	The difference between the list and the day is where the budget goes.
4	D The user's performance rating	The ledger is about the ask, not the person. It usually shows two or three asks consuming most of the budget and protecting against little.
5	C The transfer portal, which protected the plant network: the budget had been spent on prompts and timeouts that protected little, so the one that mattered was skipped	When the budget runs out, the control that fails is whichever one is next, not the least important.

#	Answer	Why
6	B Visible benefit, fast feedback, fit with the device and moment, and being asked before the control was imposed	Asks that protect nothing visible, asks that fail, and blame when the budget runs out all drain it.

Module 3: Workarounds as Data

#	Answer	Why
1	B The third response to a control that does not fit: people build their own substitute with some protection they chose, invisible to official security	From 118 interviews in one multinational. A workaround says the person wanted security and you did not give them a usable way to have it.
2	A What it keeps (the job), what it protects (the person's threat model), and what it drops (your requirement)	The redesign keeps what it keeps, protects what it protects, and adds back what it drops, in a form that costs less than the workaround did.
3	D Fix the control first, never the person; close the workaround only after a usable alternative exists and has been tested	Closing it first produces the next workaround, less visible than the last.
4	C Read helpdesk tickets for "can't", "won't let me" and "how do I get round"	Also: ask in person with no notebook, read the logs for the shape of one, ask the Champions, walk round, and make reporting one safe.
5	B Adopted the phone call as the control, removed the broken approver role, and named the people who designed it	Some workarounds are safer than the control. Adopting one, and crediting its author, brings every other workaround out of the shadows.
6	A It grew by eleven entries in a month, most of them volunteered	The line agreed with the chief operating officer: a workaround you tell us about is a design request; one we find at an incident is a conversation.

Module 4: Defaults, Paths and Friction

#	Answer	Why
1	A The step count: make the secure path the shortest one, because nobody chooses nine steps over two for a routine task and no training changes that	The portal that won was not more secure than the old one. It was shorter.
2	D Security should never compromise usability: make it secure enough, then maximise usability	The default is the strongest control you own, because most people never change one.
3	C On the rare action with a large, hard-to-reverse consequence, and on the action an attacker needs but a user seldom does	Most estates have it backwards: friction everywhere on the routine, and a rare risky action one click away.
4	B Because a block moves the workaround somewhere you cannot see it, while a slow path tells you who still needs the old way and why	Build the easy secure path, watch it win, then make the old path slow, and only then close it. Reverse the order and you get the next workaround.
5	A Pre-fill what the system already knows, put the action where the work is, replace clear-cut approvals with rules, and extend trust already established	Every step removed from the wanted action is a step you can afford to add to the unwanted one.

#	Answer	Why
6	D In month seven, after the portal had reached 310 transfers a month and USB reasons were down to three legitimate cases, all moved into the portal	Nobody noticed. The slow path had already shown that the alternative was good enough.

Module 5: Warnings, Prompts and Fatigue

#	Answer	Why
1	D About 70% in Chrome and about 33% in Firefox: the same users and threats, a different warning design	Design changed click-through by a factor of two. Malware and phishing warnings were heeded far more, which shows people are not oblivious.
2	C The brain stops processing a prompt seen often with the same safe outcome; the design built it by firing the prompt on every login, file and timeout	A security prompt answered in under a second is a reflex, and a reflex is a lever.
3	B Frequent, so users remember it	Rare, specific, consequential, actionable, safe action first. A warning the person cannot act on is noise.
4	A Because the phone asks for a number shown only on the real login screen: no number, no approval, and no reflex to exploit	A push that asks "approve?" trains approval. A prompt that asks for something only the real request has requires the real request.
5	D It becomes a one-tap report to security, and the person is thanked	If nothing happens on "no", the prompt is theatre. If a report, the prompt is a sensor.
6	C Because six seconds meant people were reading the prompt and matching the number, where under a second had been a reflex	Pushes per day fell from eleven to two, and denied prompts became reports: fourteen in the first quarter, three of them real.

Module 6: Testing a Control with Real Users

#	Answer	Why
1	C Five people who actually have the role, doing the real task on their own device in their own place, one at a time, thinking aloud, in about ninety minutes	Not their manager, not a Champion standing in, not the volunteer who likes security. The task is described as they would describe it.
2	B The usability research tradition since Nielsen: the first five find most of the serious problems and the sixth mostly repeats them; fix, then test five more	Two fix-and-retest loops is normal.
3	A A result (for example fewer than four of five completing unaided) that means the control does not ship; agreed with whoever can delay the rollout, before the test	Agreeing it afterwards means it will be negotiated away.
4	D The workaround the person tries, or says they would try, when the control does not work, written down verbatim	Also completion, time against baseline, errors, help needed and at which step, and the words they use for things.
5	C It is a hope: every control ships with one measure of the behaviour it depends on, a baseline, a workaround signal and an owner who reads it	The measure is named in the design record with the number that would mean the control has failed.

#	Answer	Why
6	B Four of the six blockers that would have reached production, including a certificate prompt nobody understood and a session that dropped when the tablet slept	After two loops: five of five unaided, task time from nine minutes to 48 seconds, and a pilot at two depots against two before rollout.

Module 7: Designing for the Moment of Attack

#	Answer	Why
1	B The attacker designs the moment, the pressure, the path and the person's state so that the easiest decision is the one they want; anything that depends on the person pausing is theirs to remove	So the pause, the check and the refusal have to be in the system, where the attacker cannot reach them. Design for the Friday brain.
2	A A hold applied by default to any payee change, with the callback number shown from the master record and a Call button on the payment screen	Five patterns: the hold, the out-of-band confirmation you control, the thing only the real request has, the four-eyes rule that works, and the cooling-off.
3	D Because at 16:40 the known channel is in a drawer and the attacker's number is on the screen; verification works when it is one tap from inside the process using nothing the request supplied	The test: could the person verify without leaving the screen, without looking anything up, and without using anything the request supplied?
4	C Not a control but a reason to bypass one; the working version is any of four named people, reachable by a route that works from a phone	The payee-change hold was used on 3% of changes until the approver step was redesigned and the hold made non-optional.
5	B Walk three ordinary people in the role through the system with the attacker's request at the worst realistic moment; if stopping it depends on one of them saying no, the control does not hold	On paper, all three finance officers paid. The hold depended on remembering it existed.
6	A Because it was built into the payment screen and applied by default, so it was not optional	Verification calls were made from the screen on 94% of changes, four minutes were added to a legitimate change, and two fraudulent changes were stopped in the first quarter.

Module 8: The Behavioural Design Record

#	Answer	Why
1	A Who the control asks, to do what, when; what it assumes about them; what it costs them; what they will do when it does not fit; whether anyone watched a real user; how we will know it works	Because the assumptions are never written down, nobody can say which one failed, and controls are re-litigated at every incident.
2	D The expected workaround: what people will do when it does not fit, by whom, how soon, and how we will see it	The seven: the ask; the actor and the moment; the COM-B dependency; the compliance cost; the expected workaround; the test; the measure and the stop number.
3	C A return, not a rejection: the design goes back for the missing piece, such as a five-user test	Within a quarter, architects start answering the six questions before they are asked. Returns at Arden fell from nine of fourteen to two of twelve.
4	B The behaviour catalogue, Champions who surface workarounds and find the five users, Team Pulse by team, and the reporting route	In return the architect gives the design record before shipping, the measure, the intervention record, and the workaround catalogue.

#	Answer	Why
5	A The behaviour the control depends on with the control's measure as a direct measure, the redesign as an intervention, the Team Pulse item and the board pack	The measure travels; the records, catalogue and logs stay with the architect.
6	D Its measure, its workaround catalogue entries and the asks-per-day count; four controls retired, including a quarterly password change and a banner nobody read	Four a year is healthy. Zero means nobody is looking.