

The First 90 Days Worksheet

What to find out, in what order, and what not to change yet.

Bhavin G Patel · C|CISO · CISSP-ISSAP · CISM

The temptation in a new security leadership role is to arrive with a plan. The plan you brought was built for a different organisation. Spend the first month finding out what is actually true, the second deciding what matters, and the third committing publicly to a small number of things you will finish.

Days 1–30 · Find out what is true

Question	Answer / who told you
What does this company actually sell, and what stops it selling?	
What is the one incident that would end careers here?	
Who owns risk acceptance, and have they ever refused anything?	
What did my predecessor promise that is still outstanding?	
Which audit or regulatory findings are open, and when are they due?	
Where is the shadow IT everyone knows about and nobody names?	
Who on the team is carrying the place, and do they know I know?	
What does the business think security does?	

CHANGE NOTHING STRUCTURAL IN MONTH ONE

Except a genuine emergency. Early reorganisations made on incomplete information cost you the credibility you will need in month six, and you cannot tell which of the odd arrangements are dysfunction and which are load-bearing until you have watched a full cycle.

Days 31–60 · Decide what matters

The three things that would hurt most

What is already good —
protect it

What is theatre and can be
stopped

The quick win that buys me
runway

What I am deliberately not
doing this year

Days 61–90 · Commit in public

- 1 **Name three outcomes for the year.** Not workstreams. Outcomes a non-security executive can tell you have or have not happened.
- 2 **Say what you are stopping.** A plan with no subtractions is not a plan, it is a wish list, and everyone in the room knows it.
- 3 **Give the honest baseline before you improve it.** The uncomfortable starting number is your best protection later: it is very hard to be blamed for a gap you documented in week ten.
- 4 **Agree how you will be measured,** with the person who will do the measuring.

Your three outcomes

THE MOST COMMON MISTAKE

Trying to fix the culture first. Culture follows repeated experience of security being useful. Deliver one thing the business actually wanted, on time, and you will get more cultural change from that than from a year of awareness campaigns.

Companion to: “Your First 90 Days as a CISO” at cybersecleader.com. Adapt freely inside your organisation with attribution retained. Not legal or regulatory advice.