

Security Programme Charter Template

A fill-in-the-blanks charter — mission, scope, authority, RACI, and a review cadence

Published 2026-09-08 · 11 minute read · For A security leader standing up (or formalizing) a programme charter for the first time

Read it now — the PDF opens either way.

Open the PDF

Leave your e-mail and we'll follow up by hand — the PDF opens either way.

you@company.com

Save my e-mail

☐ I agree to be emailed occasionally about new CMDash resources. See the [privacy policy](#).

No email — download directly

Executive summary

A programme without a charter is a pile of controls with no owner. Every other governance artefact — objectives, committees, management reviews — assumes a charter already answered “what is in scope, who runs this, and who says so.”

This template mirrors a real product, field for field. Every blank below is a field on CMDash’s own Program → Charter, Program → Objectives, and Program → Committees pages, so filling it in on paper and filling it in on screen are the same exercise.

Fill it in on paper, or skip straight to the product. Nothing below requires CMDash — a charter is a document first. Section 6 shows where each section lives if you choose to run it there.

1. Mission and scope statement

Title: _____

Mission statement — one or two sentences: why this programme exists, in the organization's own words, not a framework's.

ISMS scope statement — the boundary the rest of the programme is measured against: which business units, systems, and data are in scope.

Scope inclusions — a list: every system, business unit, or data type explicitly in scope.

Scope exclusions — a list, each entry paired with a written justification. An exclusion with no justification is the first thing an assessor questions.

2. Authority statement

One or two sentences: who grants the programme its authority — a board resolution, an executive sponsor, a specific title. This is the statement NIST SP 800-53's PM-1 control asks an information security programme plan to make, and it is what turns a charter from an aspiration into something with teeth.

Approved by: _____ Effective date: _____ Review due: _____

3. Roles: a starting RACI

A charter names who is *accountable* — one name per area, not a committee. Use this as a starting worksheet; a full RACI (adding who is Responsible, Consulted, and Informed for each area) is a planning exercise worth doing alongside it, but the Accountable column is the one a charter and an assessor both actually require.

Overall programme (the charter itself) — Accountable: _____
(starting suggestion: CISO / Head of Security)

Access control & identity — Accountable: _____ (starting suggestion: IT / Identity owner)

Incident response — Accountable: _____ (starting suggestion: Incident commander (named per Security → Incidents))

Vendor / third-party risk — Accountable: _____ (starting suggestion: Procurement or vendor-risk owner)

Data protection & privacy — Accountable: _____ (starting suggestion: DPO / privacy owner (if applicable))

Business continuity & DR — Accountable: _____ (starting suggestion: IT operations owner)

4. Objectives format

Each security objective, whether written on paper or entered into a tracker, needs the same five fields to be more than a slogan:

Title and description — what, in plain language.

Owner — one accountable person, named.

Measure and target value — the number that proves it, and the value that counts as done.

Target date and review cadence — monthly, quarterly, semiannual, or annual.

Status and status note — on track, at risk, or missed, with a sentence of why.

5. Committee terms of reference

For each standing committee (a security steering committee, an incident review board):

Name and mandate — what decisions this body actually makes.

Cadence — monthly, quarterly, semiannual, or annual.

Chair and member roster — by name and role.

Action items — tracked per meeting, each with its own owner; a committee member can close their own action item without needing to be the chair.

6. The management review cycle (ISO/IEC 27001 clause 9.3)

Top management is expected to review the ISMS at planned intervals — clause 9.3's own text is licensed and not reproduced here, but its inputs translate directly onto this charter's own artefacts: status of actions from the last review, changes in external and internal issues, performance against the objectives in section 4, audit results, and opportunities for continual improvement. Record the review's decisions and the date of the next one — a review with no recorded output is the gap an auditor finds fastest.

7. Where this runs in CMDash

Program is ungated on every CMDash plan except System Boundary, which needs Command or higher. Reading every page is open to any member; creating or editing a charter draft, objective, review, or committee is Owner or Admin.

Sections 1–2 (mission, scope, authority) — Security → Program → Charter (/program/charter). Charters are versioned; only a draft is editable.

Section 3 (accountable roles) — Security → Security Roles (/security-roles), which also runs segregation-of-duties conflict detection across who holds which role.

Section 4 (objectives) — Security → Program → Objectives (/program/objectives), linkable to specific risks and controls.

Section 5 (committees) — Security → Program → Committees (/program/committees).

Section 6 (management reviews) — Security → Program → Management Reviews (/program/reviews).

Write the charter once, reuse it everywhere

Start the first draft in Program → Charter.

30-day free trial of any paid plan (a card is required) — or sign up for Free with no card. No implementation fee.

Not ready to trial today?

Get the next paper

One email when a new white paper publishes. Nothing else.

☐ I agree to be emailed when a new CMDash white paper publishes. See the

Notify me

[privacy](#)
[policy](#)