Protect Foundations – Output Checklist

PingOne Protect

Field	Value
Version	1.0
Date	2026-04-01
Owner	Partner Delivery Architects
Intended Audience	Technical Consultants/Project Managers
Distribution	Internal/Partner

Related Delivery Kit Assets

- **Protect Foundations - Getting Started**
- **Protect Foundations - Fundamentals**
- **Protect Foundations - Best Practices**
- **Protect Foundations - PingFederate Integration Guide**
- **Protect Foundations - DaVinci Integration Guide**
- **Protect Foundations - PingAM / AIC Integration Guide**
- **Protect Foundations - Evidence Matrix Template**
- **Protect Foundations - Documentation Handover Template**

Table of Contents

Protect Foundations - Output Checklist Template

Use this checklist at project close to confirm all agreed Protect deliverables are in place, validated, and documented, ready for handover to run/ops and support. Copy this into the customer workbook or handover pack and mark each item as Complete / N/A / Follow-up.

---

1. Engagement & Scope

Confirm the engagement scope, objectives, and ownership are clearly defined and agreed with the customer.

1.1 Engagement Framing

- Engagement objectives and success criteria documented and reviewed with customer.
- In-scope user journeys listed (e.g., CIAM login, registration, recovery, workforce VPN, high-risk transactions).
- Out-of-scope items documented (deferred journeys, channels, applications).

1.2 Roles & Ownership

RACI / ownership confirmed for:

- Risk policy design and approval.
- Day-2 tuning and monitoring.
- Incident response (fraud / security).

Named owners recorded (customer + partner + Ping, where applicable).

---

2. Environment & Access

Confirm all environments, access, and credentials are correctly configured and available for ongoing operations.

2.1 PingOne Environments

- Target PingOne environments identified (DEV / TEST / PROD).
- Confirm PingOne Protect is enabled and correctly configured in all required environments.
- Worker applications created for each environment with appropriate roles.

2.2 Access & Credentials

Customer admins have access to PingOne Protect console.

Secure process agreed for managing:

- Worker app credentials.
- Any DaVinci / PF / PingAM configuration exports.

---

3. Architecture & Integration Surfaces

For each integration surface in scope, confirm that Protect is correctly implemented, integrated, and returning expected outcomes.

3.1 PingFederate (if in scope)

- PingOne Protect Integration Kit installed at required PF version.
- PingOne Protect IdP Adapter configured and tested.
- (If used) Protect Provider + device profiling templates deployed.
- PF authentication policies updated to branch on Protect risk output.

3.2 DaVinci (if in scope)

PingOne Protect connector configured (Env ID, Client ID, Client Secret).

Flows updated to:

- Create risk evaluations at appropriate decision points.
- Update risk evaluations at all end-of-flow paths.

Device/behavioural data collection implemented where required.

3.3 PingAM / AIC (if in scope)

PingOne Worker Service configured with correct environment and secret mapping.

Journeys updated with:

- PingOne Protect Initialization node.
- PingOne Protect Evaluation node.
- PingOne Protect Result node(s) at all exits.

3.4 Other Integrations (PingAccess, PingGateway, custom apps, APIs)

- Connection to PingOne Protect configured.
- Risk-based decisions wired into access / routing logic.
- Feedback (success/fail) sent back to Protect where supported.

4. Risk Policies & Predictors

Confirm risk policies and predictors are correctly configured, aligned to use cases, and appropriately tuned.

4.1 Policy Inventory

Confirm all active policies are clearly defined, mapped to journeys, and aligned to the intended use cases.

- Authentication
- Registration
- Account recovery
- High-risk transactions

Default or base policy documented and linked to relevant flows.

4.2 Predictor Usage

- Predictors in use per policy documented (including any custom predictors).
- Any third-party risk data mapped into custom attributes and predictors documented.
- Known disabled/unused predictors and rationale recorded.

4.3 Tuning State

- Training window completed for initial rollout (per use-case guidance).
- Any staging policies in use documented (with promotion plan/status).
- Known tuning decisions (threshold changes, allow lists, composites) documented with rationale.

---

5. Signals (Protect) SDK & Data Collection

Confirm device and behavioural data collection is correctly implemented, as this directly impacts risk accuracy.

5.1 Web Journeys

- Signals (Protect) SDK or equivalent JS integration deployed where required.
- Device profiling / behavioural data confirmed as present in Protect evaluations.

5.2 Mobile / Native Journeys

- Android/iOS libraries integrated and initialised correctly.
- Device identifiers mapped consistently (external device IDs, if used).

5.3 Data Quality

Confirmed:

- IP addresses reflect client, not intermediary, where required.
- User identifiers are consistent across flows.
- Any custom attributes used in predictors are reliably populated.

---

6. Validation & Testing

Confirm that Protect behaviour has been validated across expected scenarios and aligns with intended outcomes.

6.1 Functional Scenarios

Core scenarios tested and passed for each in-scope journey:

- Legitimate user (baseline).
- Legitimate user with new device.
- Higher-risk network / location (e.g., VPN, unusual geo).
- Expected bot / fraud test patterns where possible.

6.2 Risk-Based Behaviour

For each journey, documented and verified:

- What happens at **LOW** risk.
- What happens at **MEDIUM** risk.
- What happens at **HIGH** risk.

6.3 Evidence Captured

- Screenshots / exports from Threat Protection dashboard.
- Example risk evaluations (audit entries) for key scenarios.
- Confirmation that go/no-go criteria have been met, or that any exceptions have been formally reviewed and accepted.

7. Monitoring, Operations & Runbooks

Confirm the customer is able to monitor, operate, and maintain Protect independently post-handover.

7.1 Dashboards & Alerts

- Agreed views and filters in Threat Protection dashboard (per environment / journey).
- Documented KPIs to monitor (e.g., High/Medium rates, false positives, challenge/abandon rates).
- Any external monitoring / alerting hooks configured (e.g., SIEM, SOC dashboards).

7.2 Runbooks

Operations runbook for Protect (daily/weekly checks, basic triage steps).

Tuning runbook (how and when to adjust policies, review process, approvals).

Incident response outline for:

- Suspected fraud campaigns.
- System misconfiguration causing elevated false positives.

---

8. Documentation & Handover

Confirm all required documentation, artefacts, and knowledge transfer activities have been completed prior to handover.

8.1 Artefacts Included in Handover Pack

Final architecture diagram(s) showing Protect in context.

Copy or export of key configuration baselines (PF/DaVinci/AIC flows, risk policies).

Links to:

- PingOne Protect dashboards.
- Relevant Ping docs and internal references.

8.2 Handover & Ownership

- Handover session conducted with customer operations/support teams.
- Solution Handover Template completed and signed off (or equivalent).
- Open risks / follow-up items logged and assigned (with target owner and dates).

9. Sign-Off

Use this section in the customer-facing version of the checklist.

Customer Technical Owner – Name / Date
Customer Security / Risk Owner – Name / Date
Partner / Ping Delivery Lead – Name / Date

Notes / Exceptions:

Confirm all checklist items are complete.

Items with agreed exceptions listed here (including mitigation and follow-up plan).