Protect Foundations – Evidence Matrix Template

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 - Output Checklist Template**
- **Protect Foundations - Documentation Handover Template**

Table of Contents

1. Summary **3**

2. Evidence Matrix (Per Scenario) **3**

2.1 Evidence Matrix Table 4

3. Example Scenario Categories **4**

4. Protect Evidence Types **5**

5. Coverage & Gaps **5**

6. Approvals **6**

Protect Foundations - Evidence Matrix Template

Use this template to prove what was tested and how Protect behaved for each in-scope journey. It is intended to be customer-safe and to sit inside the final handover pack.

Populate one matrix per environment (e.g., TEST, PROD) or per journey group (e.g., CIAM, Workforce), depending on project size.

---

1. Summary

- **Customer / Project:**
- **Environment:** ☐ DEV ☐ TEST ☐ PROD (other:)
- **Date range of testing:**
- **Journeys covered in this matrix**
  List the journeys included in this matrix (e.g., login, registration, transactions):

---

2. Evidence Matrix (Per Scenario)

Use this table to demonstrate how Protect behaves across defined scenarios and to provide evidence that expected outcomes are achieved.

Columns (suggested):

- **ID** – Scenario identifier (e.g., AUTH-01).
- **Journey / Flow** – Login, Registration, Recovery, Transaction type, etc.
- **Channel** – Web, Mobile, API, Workforce, CIAM.
- **Scenario Description** – What is being tested.
- **Expected Behaviour** – From design / requirements (including risk expectations).
- **Protect Evidence** – What you captured (dashboard, audit, logs).
- **Status** – Pass / Fail / Not Run.
- **Notes / Defects / Follow-ups** – Any deviations, caveats, or JIRAs.

2.1 Evidence Matrix Table

Expected Behaviour (including expected risk level and outcome)

ID	Journey / Flow	Channel	Scenario Description	Expected Behaviour (incl. risk)	Protect Evidence (location / reference)	Status (Pass / Fail / N/A)

Note/Defects/Follow-ups

---

3. Example Scenario Categories

Use these example categories to ensure coverage; adapt to the project's scope.

3.1 Authentication

- AUTH-01 – Legitimate user, typical device/location, Low risk expected, frictionless path.
- AUTH-02 – Legitimate user, new device, Medium risk expected, MFA step-up.
- AUTH-03 – Suspicious IP / anonymous network, High risk expected, access denied or strong mitigation.

3.2 Registration

- REG-01 – Legitimate registration with normal email, Low risk, account created.
- REG-02 – Disposable/temporary email, mitigation applied (TEMP_EMAIL_MITIGATION), registration blocked or flagged.
- REG-03 – High-volume/bot-like registration attempt, High risk, mitigated/blocked.

3.3 Account Recovery

- REC-01 – Legitimate recovery from normal context, acceptable risk, recovery succeeds.
- REC-02 – Recovery from unusual location/device following failed login, High risk, routed to manual or strong recovery path.

3.4 High-Risk Transactions

- TX-01 – Low-value transaction, Low risk, minimal friction.
- TX-02 – High-value transaction, Medium/High risk, MFA/step-up enforced.
- TX-03 – Suspicious device or behaviour, High risk, transaction denied.

(These are suggestions; adjust to your agreed scope.)

---

4. Protect Evidence Types

Use consistent evidence types to ensure scenarios can be reviewed and validated easily by stakeholders.

Indicate what forms of evidence are captured for each scenario. You can use these as tags in the **Protect Evidence** column.

- **TP-DASH** – Threat Protection dashboard screenshot (with filters/date range visible).
- **TP-AUDIT** – Audit log entry (Risk Evaluation Created / Updated), with key fields.
- **CFG-POLICY** – Screenshot or export of the relevant risk policy.
- **CFG-FLOW** – Screenshot or export of the relevant PF/DaVinci/PingAM journey or flow.
- **LOG-APP** – Application / gateway logs confirming end-to-end behaviour.

Example Protect Evidence cell:

```
TP-DASH #1; TP-AUDIT RE-12345; CFG-POLICY Auth-Base v1.2
```

---

5. Coverage & Gaps

Summarise overall test coverage and highlight any gaps that may impact confidence in the solution.

5.1 Coverage Summary

- Total scenarios defined:
- Scenarios executed:

- Scenarios passed:
- Scenarios failed (open):

5.2 Known Gaps / Out-of-Scope

Certain journeys not tested (list which and why).
Environments where testing is incomplete or not performed.
Predictors/policies not exercised in this phase (e.g., some high-risk transaction cases).

---

6. Approvals

Use in the customer-facing version.

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

Comments: