



See the estate the way the decision needs it

A useful inventory is scoped to a named site, service, run and collection boundary. It shows what was observed, how identity was inferred and what the collector could not see.

Observed

Assets, services and evidence accepted into the named run.

Uncertain

Weak identities, unmatched records and missing coverage remain visible.

Owned

Every important unknown becomes a question for a named site or service owner.

What changes for management

The team stops arguing about inventory totals and starts asking which observations support a service decision.

Proof to ask for

Run identity, collector vantage point, enabled methods, timestamps and visible gaps.

Boundary to retain

A collector can only report what its placement and supported methods allow it to observe.

Outcome: The team agrees which part of the estate is known well enough to review and which gap must be closed next.



Give every device an evidence-backed passport

The device passport connects identity, source, time, services and confidence. Similar records can be organized in batches, while outliers and weaker evidence remain separate.

Identity

Why the record describes this device.

Context

What the device supports and which services are exposed.

Coverage

Which methods ran, from which vantage point, and what remains unseen.

What changes for management

A familiar device name becomes a reviewable identity with a reason to trust it and a reason to check it.

Proof to ask for

Source observations, identity confidence, service context and the outliers excluded from any batch decision.

Boundary to retain

A repeated pattern can organize work; it does not prove every device identity or exposure.

Outcome: The owner can defend the device identity while keeping weaker records and exceptions visible.



Prioritize exposure without overstating it

Secure brings software, candidate vulnerabilities, planning examples and possible attack routes into one review. Each keeps its own evidence boundary.

Candidate

A database or model match deserves investigation.

Confirmed

A reviewer has checked applicability within the recorded scope.

PQC planning

Use labeled examples to frame role, lifetime, dependencies and ownership; they are not a customer assessment.

What changes for management

Severity and route diagrams become questions for investigation instead of conclusions presented as facts.

Proof to ask for

Applicability checks, source context, reviewer rationale and the evidence that would change the priority.

Boundary to retain

PQC workspace examples are planning simulations, not customer cryptographic assessments.

Outcome: The next investigation is prioritized by evidence, business context and uncertainty rather than a score alone.



Leave the owner with a scoped plan

Compare the next run with the prior evidence, preserve rationale, and recheck changed identity, firmware, exposure and cryptography before expanding scope.

Collect

Place authorized collection where it can answer the question.

Review

Retain evidence, uncertainty and exceptions.

Decide

Expand, narrow, pause or stop with an accountable owner.

What changes for management

The owner receives a decision record that can be rechecked when the estate or collection window changes.

Proof to ask for

Earlier rationale, current evidence, changed assets, current owner and the next review date.

Boundary to retain

A new run does not automatically inherit an earlier acceptance or validation decision.

Outcome: The pilot closes with a scoped operating decision and an accountable owner for every remaining gap.