# Security Roadmap Workshop

## Introduction & Purpose

This workshop helps organisations translate security posture assessments into a pragmatic, executive-aligned roadmap. Using findings from previous engagements—like Sensitivity Labelling, DLP, Essential 8 assessments, or Secure Score—the workshop prioritises improvements in a *Crawl–Walk–Run* framework.

**This is not** a detailed implementation workshop. Its goal is to align stakeholders on what matters most now, clarify strategic priorities, and produce a phased plan that mitigates risk effectively while enhancing maturity and compliance.

## Rules of Engagement

E2’s charter ensures customers feel knowledgeable and confident in planning secure digital offerings.

* **Executive focus**: Speak business outcomes — such as uptime, regulatory compliance, data protection — not technical configuration.
* **Structured consensus**: Use the Crawl–Walk–Run model to build alignment and show short-, mid-, and long-term goals.
* **Capture, don’t dive**: If debate goes deep into implementation details, note it for follow-up reference.
* **Adaptable and simple**: Ensure the roadmap is realistic and achievable; customers must walk away with confidence in execution.
* **Do not prescribe solutions**—recommend principle-based improvements, not canned technology choices.

## Step-by-Step Delivery

### Step 1 – Set the Scene & Context

* Recap previous assessments and security posture.
* Confirm workshop objectives: clarity of roadmap, alignment of priorities, timeline agree-up.
* Identify stakeholders and decision-makers in the room.

### Step 2 – Review Maturity Snapshot

* Walk through current maturity levels (Essential 8, Labeling, DLP, Secure Score).
* Clarify major gaps, controls in place, and risk exposure.

### Step 3 – Crawl Phase (Immediate Wins)

* Identify quick uplift opportunities achievable within 1–2 weeks (e.g. enforce MFA, disable macros, apply baseline DLP).
* Confirm ownership and how to measure short-term success.

### Step 4 – Walk Phase (Mid-Term Projects)

* Define mid-term initiatives (30–90 days) like auto-label deployment, roadmap delivery, Secure Score improvement projects, remediation of architectural gaps.
* Prioritise by risk, cost, and business value.

### Step 5 – Run Phase (Strategic Transformation)

* Discuss long-term strategic security projects (e.g. Identity Governance, IRM, Sentinel/ XDR rollout).
* Define funding/approval horizon, KPIs, and executive sponsorship requirements.

### Step 6 – Align Timeline & Owners

* Build a visual roadmap timeline (e.g. Gantt or bar view).
* Assign executive sponsors, operational leads, and review cadence.

## Engagement Outputs

By session close, deliverables include:

* A **phased roadmap** (Crawl–Walk–Run) with high-level milestones and owners.
* A one-page **executive summary** (heat-mapped maturity and key initiatives).
* A **quick-win tracker** (who, what, by when).
* A **mid-term project bundle** with outcome expectations.
* A **strategic transformation outline** (with anticipated funding needs and business impact).

## References & Learning Resources

* **Microsoft Zero Trust Workshop Guidance (Roadmap tool)**  
  Template platform for mature roadmap tracking and status monitoring :contentReferenceoaicite:2
* **ACSC Essential 8 Maturity Model** – Align quick wins and mid-term improvements across RTO, integrity, and patching maturity :contentReferenceoaicite:3
* **Crawl–Walk–Run Security Uplift Model** – Industry-proven approach to incremental maturity.
* **Microsoft Learn: Secure Score Improvement** – Plays into roadmap actions and time-bound progress tracking.