Title

Maturion Operational Maturity House – Domain-Level Hover Content (Marketing Mode)

Category

Policy Model

Description

Structured content for **Marketing/Demo Mode** on the **/demo** page.

Defines hover logic and AI assistant responses for **Domain-level** explanations at **each Maturity Level**.

Supports *sales-focused education*, *conversion*, and *future assessment criteria automation*.

Tags

maturity model, hover logic, AI guidance, marketing, domain-level, free assessment, subscription, APGI certification, sales conversion

---

Upload Notes (Admin Only)

This content is for the **Operational Maturity House** on the **public-facing /demo page**.

It supports:

- Domain-level hover interactivity *within* each Maturity Level.
- Sales-focused education to help prospective customers understand specific weaknesses and improvement steps.
- Maturion AI chatbot training to answer granular questions about *any Domain at any Level*.
- Future scaling to *Assessment Criteria* with evidence expectations per Level.

Body Content

✅ Instructions for AI

When a user is on the **/demo page** and:
✅ Clicks on a **Maturity Level** (e.g., Basic) → The House locks to that level.
✅ Now each **Domain** is hoverable.

✅ On hover over a **Domain**:

- **Left Panel:** *What this Domain looks like at this Level.*
- **Right Panel:** *What needs to be done in this Domain to move to the next Level.*

✅ **AI must:**
✔ Provide clear, professional, and sales-focused text.
✔ Emphasise best practices, international standards.
✔ Use language that educates and motivates.
✔ Always encourage the **Free Assessment**.
✔ Be ready to help user understand how APGI Certification supports this journey.

✅ Structured Content Example

Below is a **sample structure** Maturion will use to serve hover responses.

Level: Basic

✅ **Domain: People and Culture**

- **Left Panel:**

  "At Basic, People and Culture is informal and unstructured. Roles and responsibilities are unclear, accountability is limited, and security awareness is minimal."

- **Right Panel:**

  "Define clear roles and responsibilities. Introduce basic security training. Establish onboarding that includes security expectations. Build a security-conscious culture."

✅ **Domain: Process Integrity**

- **Left Panel:**

  "Process Integrity at Basic means workflows are undocumented and vary between individuals or departments. Controls are inconsistent and risk is unmanaged."

- **Right Panel:**

  "Document standard operating procedures. Train staff to follow consistent workflows. Assign responsibility for maintaining and improving processes."

✅ **Domain: Protection**

- **Left Panel:**

  "Protection at Basic is reactive. Physical and technical controls are minimal, informal, or outdated. Access is poorly controlled."

- **Right Panel:**

  "Assess site security needs. Implement basic access control measures. Establish visitor logs. Begin securing sensitive areas."

✅ **Domain: Proof**

- **Left Panel:**

  "Proof at Basic lacks documentation. There is no reliable evidence of compliance or controls, making external assurance impossible."

- **Right Panel:**

  "Start capturing simple records. Store documents in a consistent, secure way. Train staff on why evidence is important."

Level: Reactive

✅ **Domain: People and Culture**

- **Left Panel:**

"At Reactive, people respond to issues as they arise. Security training is ad hoc. Accountability exists only after problems occur."

- **Right Panel:**

  "Introduce scheduled security training. Clarify escalation procedures. Build feedback loops to learn from incidents."

✅ **Domain: Process Integrity**

- **Left Panel:**

  "Processes are partly documented but often ignored. Responses are event-driven without root cause analysis."

- **Right Panel:**

  "Formalise workflows. Introduce risk assessments. Implement incident logging and analysis to learn from failures."

✅ **Domain: Protection**

- **Left Panel:**

  "Controls are upgraded only after incidents. Security improvements are ad hoc."

- **Right Panel:**

  "Conduct formal site assessments. Develop a proactive security plan. Prioritise improvements based on risk."

✅ **Domain: Proof**

- **Left Panel:**

  "Evidence is collected inconsistently, often after problems occur. Records are incomplete or hard to find."

- **Right Panel:**

  "Standardise incident logging. Store records securely. Review documentation regularly for accuracy."

Level: Compliant

✅ Domain: People and Culture

- **Left Panel:**

  "Roles and responsibilities are formally defined. Training exists but may not cover all risks or be consistently delivered."

- **Right Panel:**

  "Integrate training into onboarding. Schedule regular refreshers. Build a strong reporting culture with clear expectations."

✅ Domain: Process Integrity

- **Left Panel:**

  "Standard operating procedures are in place but may not be consistently followed. Controls meet minimum requirements."

- **Right Panel:**

  "Embed continuous improvement. Use audits and reviews to close gaps. Train teams on consistent compliance."

✅ Domain: Protection

- **Left Panel:**

  "Controls meet regulatory or contractual minimums. Coverage may be siloed or outdated."

- **Right Panel:**

  "Integrate systems. Update technology. Build layered, risk-based protection aligned to best practices."

✅ Domain: Proof

- **Left Panel:**

  "Records are available but may be incomplete or inconsistent. External audits are challenging."

- **Right Panel:**

  "Implement audit-ready documentation. Train staff on evidence standards. Automate record-keeping where possible."

Level: Pro-active

✅ **Domain: People and Culture**

- **Left Panel:**

  "Security culture is strong. Risks are anticipated. Staff are empowered but may need more automation and analytics."

- **Right Panel:**

  "Automate training tracking. Use surveys and feedback. Benchmark against industry standards."

✅ **Domain: Process Integrity**

- **Left Panel:**

  "Workflows are consistent and measured. Improvements happen regularly, driven by incident analysis."

- **Right Panel:**

  "Introduce advanced analytics. Automate monitoring. Integrate with risk management frameworks."

✅ **Domain: Protection**

- **Left Panel:**

  "Controls are consistent and risk-based. Technology is integrated. Reviews are regular."

- **Right Panel:**

  "Expand advanced detection systems. Integrate with emergency response. Embed supply chain security."

✅ **Domain: Proof**

- **Left Panel:**

  "Evidence is reliable and audit-ready. Monitoring is structured but may lack real-time capabilities."

- **Right Panel:**

  "Implement live dashboards. Use real-time alerts. Integrate with remote assurance and independent reviews."

Level: Resilient

✅ **Domain: People and Culture**

- **Left Panel:**

  "Highly security-conscious, trained, and accountable teams. Leadership models commitment."

- **Right Panel:**

  "Maintain advanced training. Sustain security culture. Share learnings across the organisation."

✅ **Domain: Process Integrity**

- **Left Panel:**

  "Processes are optimised, adaptive, and continuously improving. Risk assessments are dynamic and embedded."

- **Right Panel:**

  "Review emerging risks. Integrate with global best practices. Sustain evidence-based improvements."

✅ **Domain: Protection**

- **Left Panel:**

  "Layered, risk-based controls. Advanced technology. Trusted by stakeholders."

- **Right Panel:**

  "Continually evaluate new threats. Invest in innovation. Maintain stakeholder confidence."

✅ **Domain: Proof**

- **Left Panel:**

  "Fully integrated, secure, and audit-ready systems. Supports remote, independent assurance."

- **Right Panel:**

  "Automate audits. Enable real-time assurance. Use analytics to identify improvements and risks."

✅ **General CTA Below House:**

"**Ready to see where your organisation stands? Start your Free Assessment today and unlock your personalised roadmap to Operational Excellence.**"
[**Take Free Assessment** Button]

✅ **Admin Notes (For Lovable Team):**

This structured content is for **Domain-level hover logic** when a Maturity Level is selected on the **/demo** page.
Must support:

- Click Level → Lock House.
- Hover Domain → Show Left/Right Panels.
- Consistent, sales-friendly, best-practice messaging.
- Editable in AI Back Office for easy updates.

- Maturion Assistant must respond using this logic in chat.

✅ **Verdict:**
This upload gives **AI-ready structured content** for Domain-Level hover behavior on the demo page, setting the foundation for **assessment criteria guidance** in future phases.