

OWASP LLM Top 10 × Mycelium 14-Dimension Framework.

Twelve LLM-specific threats. Where each one lives in the governance and operations stack.

T H E T E N T H R E A T S

- LLM01
Prompt injection
- LLM02
Sensitive info disclosure
- LLM03
Supply chain
- LLM04
Data / model poisoning
- LLM05
Improper output handling
- LLM06
Excessive agency
- LLM07
System prompt leakage
- LLM08
Vector / embedding weaknesses
- LLM09
Misinformation / hallucination
- LLM10
Unbounded consumption

DIM	DIMENSION	LLM01	LLM02	LLM03	LLM04	LLM05	LLM06	LLM07	LLM08	LLM09	LLM10
D01	Strategy & alignment										
D02	Accountability & ownership						✓				
D03	Risk appetite & tolerance										
D04	Model governance			✓	✓				✓		
D05	Vendor & third-party governance			✓							
D06	Data governance & protection		✓		✓	✓			✓		
D07	Model security & integrity	✓			✓			✓			
D08	Identity & access management						✓	✓			
D09	Supply chain & tooling security			✓							
D10	Monitoring & observability	✓								✓	✓
D11	Incident response & recovery	✓				✓				✓	
D12	Change & release management			✓	✓						
D13	Capability & skills										
D14	Culture & awareness									✓	

L E G E N D

✓ PRIMARY — control lives natively in this dimension

✓ SUPPORTS — dimension co-delivers the control

Threat-by-threat. Every LLM-class vulnerability has a named dimension. themyceliumgroup.com.au

The dimensions that stay blank (Strategy · Risk appetite · Capability) are not gaps. They are reminders that controls without governance fail differently.