CASF(TM) Foundations framework crosswalk

CASF(TM) Foundations · alignment evidence, not a seal · v2026-11-05

Curriculum alignment only. Not an endorsement by NIST, ISO, the European Union, or OWASP. Not ANAB / ISO/IEC 17024, not NICCS, not government-recognized, not legal advice, and not an official EU certificate. CASF(TM) Foundations is a professional certificate issued by Gabby Software Engineering LLC.

Module	NIST AI RMF function	ISO/IEC 42001 theme	EU AI Act article	OWASP Top 10 for LLMs
M0 Why AI Safety Is Not Security	Map - context and risk framing (safety vs security)	Context of the organization; intended use of AI	Art. 4 AI literacy - know the kind of risk; not a high-risk conformity claim	Threat-side contrast: LLM01 Prompt Injection vs accidental harm
M1 How AI Can Fail You	Map + Measure - failure modes and a starter risk register	Planning / AI risk assessment (theme, not a full Clause 6 implementation)	Deployer risk awareness (Art. 26 themes); not provider Art. 9 risk management	LLM02 Insecure Output Handling; LLM09 Overreliance
M2 Truth & Bias	Measure - truth, hallucination, and bias	Impacts on people; accuracy and fairness as risk themes	Transparency duties (Art. 13 / Art. 50 themes) when people interact with AI	LLM09 Overreliance - treating invented output as fact
M3 Privacy & Confidentiality	Map - data and context; Measure - leakage	Operational data controls; documented information	Deployer confidentiality practice (not a GDPR or official EU certificate)	LLM06 Sensitive Information Disclosure
M4 Accountability & Law	Govern - roles, oversight, and literacy	Leadership, roles, and competence	Art. 4 literacy; Art. 14 human oversight; Art. 26 deployer obligations (plain English)	Human review against LLM09 Overreliance
M5 Ship It: Final Policy	Govern + Manage - written policy and a review path	Documented AI policy / management-system alignment	Literacy and deployer evidence you can show - not an official EU certificate	M0-M4 controls written into one workplace policy

M6 is the identity-verified exam of M0-M5. It does not add a new framework mapping.

Live page: https://www.getaisafetycertified.com/framework-crosswalk