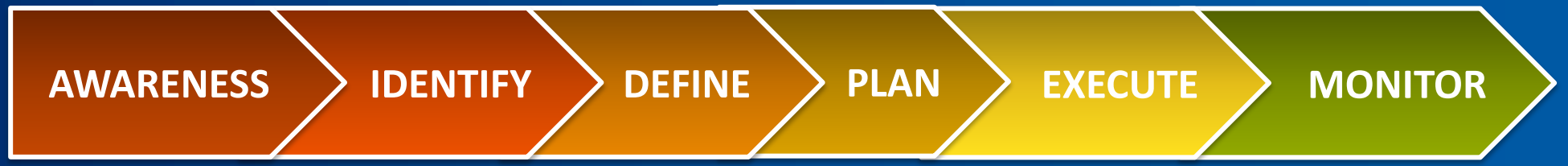

CERTFin

- **Consapevolezza**: Questa fase mira ad allineare il top management , condividendo tutti quegli elementi utili a comprendere i rischi associati a una gestione tardiva delle potenziali problematiche.
- **Identificazione** (o Discovery): Identificare tutte le aree in cui gli algoritmi di crittografia sono utilizzati (sw, hw e servizi) internamente all'azienda e da terze parti. L'obiettivo principale è quello di costruire un ***crypto-inventory*** consultabile e sempre aggiornato che permetta di individuare dove intervenire e con quale impatto nel caso in cui sia necessario sostituire un algoritmo crittografico.
- **Definizione** (o Preparazione): Questa fase si concentra sulla definizione della strategia degli obiettivi, sulla costruzione di una roadmap, sulla stima del budget necessario, sulla costituzione del gruppo di lavoro, ecc. È essenziale concentrare le aspettative sul breve, medio e lungo termine.
- **Pianificazione**: In questa fase, gli interventi vengono pianificati in linea con un «***Quantum Threat model***» per stabilire le priorità degli interventi. È essenziale concentrarsi sulla durata di vita dei dati (ad esempio, potrebbe non essere necessario proteggere un contratto che dura un anno).
- **Esecuzione**: Attività che possono spaziare dalla logica ibrida alla logica interamente post-quantistica. Un aspetto da privilegiare è la messa a punto di sistemi ***crypto-agili***.
- **Monitoraggio**: verificare, in modo continuato, che gli algoritmi utilizzati siano ancora considerati affidabili, sicuri e performanti.